BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

BL

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-148924

(43)Date of publication of application : 30.05.2000

(51)Int.Cl. G06K 17/00
G06F 12/14
G06F 17/30
G06K 19/10

(21)Application number : 11-311384

(22)Date of filing : 28.09.1999

(71)Applicant : NCR INTERNATL INC

(72)Inventor : O'FLAHERTY KENNETH W
WATTS REID M
RAMSAY DAVID A

(30)Priority

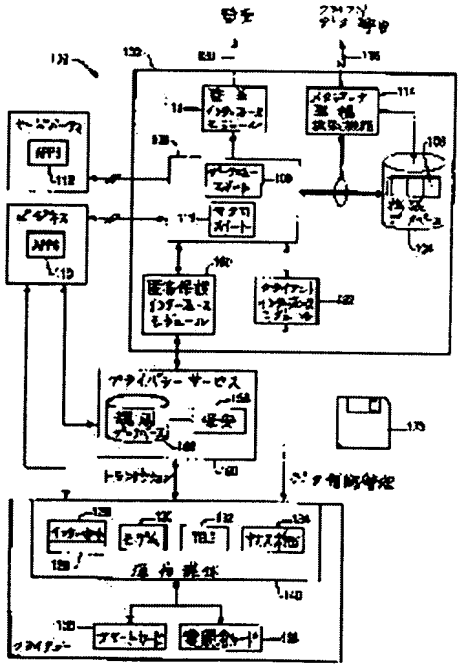
Priority number : 98 165457 Priority date : 02.10.1998 Priority country : US

(54) CARD SYSTEM IMPROVING PRIVACY PROTECTION FUNCTION

(57)Abstract:

PROBLEM TO BE SOLVED: To give the entire advantages of a complete data warehouse by receiving a request from a consumer, asking the consumer for consumer information, etc., storing a proxy which identifies the customer and is proper to the customer in the data warehouse and issuing a privacy card.

SOLUTION: First, a request for a consumer privacy card such as a favorer card 138 or a smart card 136 is received from a customer. This is accomplished via the Internet 126 performed through a modem 130, telephone 132 or a kiosk/ ATM 134. Next, the consumer receives interrogating for obtaining consumer information and privacy preference. Then, a proxy proper to the customer which identifies the customer is generated, is associated with the personal information of the customer and is stored in a data warehouse. And, a privacy card that expresses the privacy preference of the customer clearly is issued.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－148924
（P2000－148924A）
(43)公開日　平成12年５月30日(2000.5.30)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ	17/00	Ｂ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ａ
17/30			15/40	３２０Ｂ
Ｇ０６Ｋ　19/10			15/401	３２０Ｚ
		Ｇ０６Ｋ	19/00	Ｒ

審査請求　未請求　請求項の数22　ＯＬ　外国語出願　（全 63 頁）

(21)出願番号　特願平11－311384

(22)出願日　平成11年９月28日(1999.9.28)

(31)優先権主張番号　０９／１６５４５７

(32)優先日　平成10年10月２日(1998.10.2)

(33)優先権主張国　米国（ＵＳ）

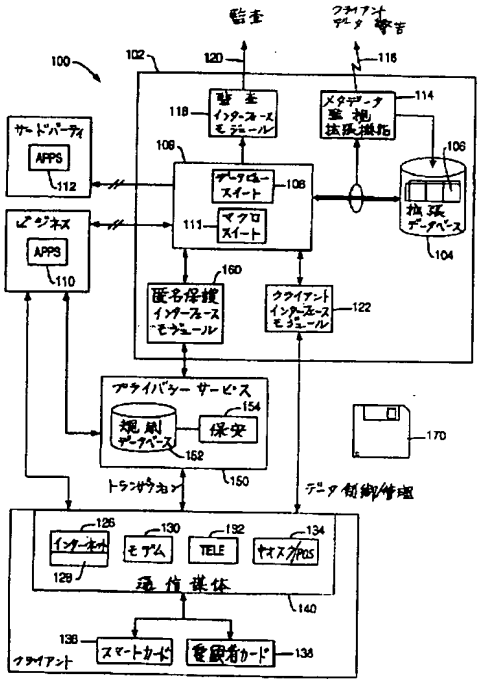
(71)出願人　592089054
エヌシーアール　インターナショナル　インコーポレイテッド
ＮＣＲ　Ｉｎｔｅｒｎａｔｉｏｎａｌ，Ｉｎｃ．
アメリカ合衆国　45479　オハイオ、デイトン　サウス　パターソン　ブールバード　1700

(74)代理人　100098589
弁理士　西山　善章

最終頁に続く

(54)【発明の名称】　プライバシー保護機能を向上させたカードシステム

(57)【要約】
【目的】　データウェアハウスに格納されているデータの収集および配布を制御するための装置、製造品、及びメモリ構造を提供する。
【構成】　本方法は、プライバシーカードを求めるリクエストを消費者から受け取るステップと、消費者に消費者情報及びプライバシープレファレンスを問い合わせるステップと、顧客を同定する顧客固有プロキシをデータウェアハウスに格納するステップと、そのプロキシを含むプライバシーカードを当該顧客に発行するステップとを含む。本プログラム格納装置は上述の方法を実行する命令を格納する媒体を含む。本装置は消費者からプライバシーカードを求めるリクエストを受け取ると共に該消費者に消費者個人情報及びプライバシープレファレンスを問い合わせるための、キオスク、ＡＴＭあるいはインターネット接続装置等の手段と、顧客の固有のプロキシを格納する該データウェアハウスと、プライバシーカードを発行する手段とを含む。



1

【特許請求の範囲】

【請求項１】プライバシーカードを求めるリクエストを消費者から受け取るステップと、
該消費者に消費者情報およびプライバシープレファレンスを問い合わせるステップと、
該顧客を同定する顧客固有プロキシを該データウェアハウスに格納するステップと、
該プロキシを含むプライバシーカードを該顧客に発行するステップとを含むことを特徴とするデータウェアハウスに格納されているデータの収集および配布を制御する方法。

【請求項２】顧客固有プロキシをデータウェアハウスに格納する該ステップが、
該プロキシを発生するステップと、
該顧客固有プロキシを該データウェアハウスに格納するステップと、
該プロキシを該プライバシーカードに格納するステップとを含むことを特徴とする請求項１に記載の方法。

【請求項３】該プライバシーカードがスマートカードであることを特徴とする請求項２に記載の方法。

【請求項４】顧客固有プロキシをデータウェアハウスに格納する該ステップが、
該プライバシーカードから該プロキシを読み取るステップと、
該プロキシを該データウェアハウスに格納するステップとを含むことを特徴とする請求項１に記載の方法。

【請求項５】該プロキシを含んだ商取引を求めるリクエストを該消費者から受信するステップと、
該商取引に関するデータを該プロキシに関連づけるステップと、
該関連づけた該商取引データを該データウェアハウスに格納するステップとをさらに含むことを特徴とする請求項１に記載の方法。

【請求項６】該データウェアハウス内のプライバシープレファレンスを管理するためのリクエストを該消費者から受信するステップと、
該消費者の身元を照合確認するステップと、
消費者プライバシープレファレンス管理命令に従って該データウェアハウスに格納されている該プライバシープレファレンスを管理するステップとをさらに含むことを特徴とする請求項１に記載の方法。

【請求項７】該プロキシが、該消費者個人情報からとは別に安全に該データウェアハウスに格納されることを特徴とする請求項１に記載の方法。

【請求項８】複数の小売業者各々に対して消費者固有同定コードが発生され格納されることを特徴とする請求項１に記載の方法。

【請求項９】プライバシーカードを求めるリクエストを消費者から受け取る手段と、
該消費者に消費者個人情報およびプライバシープレファレンスを問い合わせる手段と、
該顧客を同定する顧客固有プロキシを該データウェアハウスに格納する手段と、
該プロキシを含むプライバシーカードを該顧客に発行する手段とを含むことを特徴とするデータウェアハウスに格納されているデータの収集および配布を制御する装置。

2

【請求項１０】顧客固有プロキシをデータウェアハウスに格納する該手段が、
該プロキシを発生する手段と、
該顧客固有プロキシを該データウェアハウスに格納する手段と、
該プロキシをプライバシーカードに格納する手段とを含むことを特徴とする請求項９に記載の装置。

【請求項１１】該プライバシーカードがスマートカードであることを特徴とする請求項１０に記載の装置。

【請求項１２】顧客固有プロキシをデータウェアハウスに格納する該手段が、
該プライバシーカードから該プロキシを読み取る手段と、
該プロキシを該データウェアハウスに格納する手段とを含むことを特徴とする請求項９に記載の装置。

【請求項１３】該プロキシを含んだ商取引を求めるリクエストを該消費者から受信する手段と、
該商取引に関するデータを該プロキシに関連づける手段と、
該関連された該商取引データを該データウェアハウスに格納する手段とをさらに含むことを特徴とする請求項９に記載の装置。

【請求項１４】該データウェアハウス内のプライバシープレファレンスを管理することのリクエストを該消費者から受信する手段と、
該消費者の身元を照合確認する手段と、
消費者プライバシープレファレンス管理命令に従って該データウェアハウスに格納されている該プライバシープレファレンスを管理する手段とをさらに含むことを特徴とする請求項９に記載の装置。

【請求項１５】該プロキシが、該消費者個人情報からとは別に安全に該データウェアハウスに格納されることを特徴とする請求項９に記載の装置。

【請求項１６】複数の小売業者各々に対して消費者固有同定コードが発生され格納されることを特徴とする請求項９に記載の装置。

【請求項１７】コンピュータで読み取り可能なプログラム格納装置にしてデータウェアハウスに格納されているデータの収集および配布を制御する方法を実行するための、該コンピュータにより実行可能な一つ以上の命令を具備しているプログラム格納装置であって、該制御する方法において、
プライバシーカードを求めるリクエストを消費者から受

け取るステップと、
該消費者に消費者情報およびプライバシープレファレンスを問い合わせるステップと、
該顧客を同定する顧客固有プロキシを該データウェアハウスに格納するステップと、
該プロキシを含むプライバシーカードを該顧客に発行するステップとを含むことを特徴とするプログラム格納装置。
【請求項１８】該顧客固有プロキシをデータウェアハウスに格納する該ステップが、
プロキシを発生するステップと、
該顧客固有プロキシを該データウェアハウスに格納するステップと、
該プロキシをプライバシーカードに格納するステップとを含むことを特徴とする請求項１７に記載の装置。
【請求項１９】該プライバシーカードがスマートカードであることを特徴とする請求項１８に記載の装置。
【請求項２０】顧客固有プロキシをデータウェアハウスに格納する該方法が、
該プライバシーカードから該プロキシを読み取るステップと、
該プロキシを該データウェアハウスに格納するステップとを含むことを特徴とする請求項１７に記載の装置。
【請求項２１】該方法が、
該プロキシを含んだ商取引を求めるリクエストを該消費者から受信するステップと、
該商取引に関するデータを該プロキシに関連づけるステップと、
該関連づけた商取引データを該データウェアハウスに格納するステップとをさらに含むことを特徴とする請求項１７に記載の装置。
【請求項２２】該方法が、
該データウェアハウス内のプライバシープレファレンスを管理するためのリクエストを該消費者から受信するステップと、
該消費者の身元を照合確認するステップと、
消費者プライバシープレファレンス管理命令に基づき該データウェアハウスに格納されている該プライバシープレファレンスを管理するステップとをさらに含むことを特徴とする請求項１７に記載の装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明はデータのウェアハウス（倉庫）化および解析の方法およびシステムに関し、特にデータベース管理システムにプライバシー制限を課する方法および装置に関する。
【０００２】
【従来の技術】データベース管理システムはデータを収集、流布、および解析するのに使われる。このような大規模統合データベース管理システムは大量のデータを格

納し、取出し、解析するための、効率的で一貫したかつ安全にデータのウェアハウス化を行う能力を提供する。大量の情報を収集、解析および管理を行うこの能力は、今日のビジネス界においてほぼ必須のものとなっている。
【０００３】これらのデータウェアハウスに格納される情報は種々のソースから到来しうる。一つの重要なデータウェアハウス化アプリケーションはビジネス機関と消費者との間の商取引の過程で収集される情報の収集および解析を行う。例えば、ある個人が小売店である物品を購入するためにクレジットカードを使用すると、顧客の同定、購入物品、購入額その他の関連情報が収集される。従来、このような情報は当該取引を完了すべきか否かを決定するため、および製品在庫を制御するために小売業者が使用している。そのようなデータはまた、現在の購入傾向および地域的購入傾向を決定するのにも使用することができる。
【０００４】他の産業界でも個人データの使用が同様に行われている。例えば、銀行業務においては顧客の購買パターンはそのクレジットカード取引プロファイルまたは当座／預金口座の活動を解析することにより予測することができ、またある種のプロファイルをもつ顧客達は抵当や個人的退職者口座のような新規サービスを求める潜在的顧客として同定することができる。さらに、通信産業界では、通話記録から消費者通話パターンを解析することができ、ある種のプロファイルをもつ個人を２本目の電話線あるいはコールウェイテシングのような更なるサービスの販売の対象として特定することができる。
【０００５】さらに、データウェアハウス保有者は、普通、取引データを豊富にするためのデータをサードパーティー（第三者）から購入する。この豊富化のプロセスは家族構成員の会員権、収入、雇用主、その他の個人データなどの人口統計データを豊かにする。
【０００６】そのような取引期間中に収集されたデータは他の用途にも有用である。例えばある特定の取引に関する情報は当該消費者についての個人情報（年齢、職業、住居地、収入等）に相関づけて統計的情報を発生させることができる。ある場合にはこの個人情報は大まかに、当該消費者の身元（identification）を表す情報とそうでない情報との二つのグループに分類することができる。消費者の身元を表さない情報は有用である。なぜならばそれが類似の個人的特徴をもつ消費者達の購入傾向に関する情報を得るのに使用することができるからである。消費者の身元を表す個人情報はより絞り込んだ個人的市場戦略に使用することができる。その場合、各個人消費者の購入習慣が解析されて別の市場の候補者あるいはある好みに合わせて手直しした市場の候補者が同定される。
【０００７】個人データの収集が増大している別の例は、最近の「会員制」カードあるいは「愛顧者」カード

5

の繁栄に現れている。これらのカードはある種の製品について顧客に割引価格を提供する。しかし顧客がそのカードを購入に使用する度に、顧客の購入習慣に関する情報が収集される。オンライン環境あるいはスマートカード、電話カードおよび借入カードすなわちクレジットカードでも同じ情報が得られる。

【０００８】そのようなデータの収集および解析が大きな大衆的利益になりうるものの、それは残念ながらかなり悪用の対象ともなりうる。愛顧者プログラムの場合、かかる悪用の可能性が、本来は協力的な多数の消費者が会員賞やその他のプログラムを得るのに参加することを阻害しかねない。またかかる悪用はキャッシュカードのような将来的技術を使用することを拒ませ、現金および小切手のようなより保守的な支払方法を継続することを助長する。実際、プライバシーに関する公衆の心配が、ウェブ商業が爆発的成長するとの期待を遅らせている要因であると信ぜられる。

【０００９】これらすべての理由から、通常の制約と同様、個人情報がデータウェアハウスに格納されるとき、データを制御する者達はそのような悪用からデータを保護することを要求される。このコンピューター時代にあって、データが益々収集されるにつれて個人に関するデータの使用上、個々人の権利が益々重要になっている。

【００１０】

【発明が解決しようとする課題】本発明は、消費者のプライバシー保護の要望に応えつつ完全なデータウェアハウスのすべての利点を与えるシステムおよび方法を与えることを目的とする。

【００１１】

【課題を解決するための手段】第一の局面から見ると、本発明はデータウェアハウスに格納されているデータの収集および配布を制御する方法であって、プライバシーカードを求めるリクエストを消費者から受け取るステップと、該消費者に消費者情報およびプライバシープレファレンスを問い合わせるステップと、該顧客を同定する顧客に固有なプロキシ（以下、顧客固有プロキシという）を該データウェアハウスに格納するステップと、該プロキシを含むプライバシーカードを該顧客に発行するステップとを含むことを特徴とする方法に実現される。

【００１２】第二の局面からみると、本発明はデータウェアハウスに格納されているデータの収集および配布を制御する装置であって、消費者からプライバシーカードを求めるリクエストを受け取る手段と、該消費者に消費者の個人情報（以下、消費者個人情報という）およびプライバシープレファレンス（privacy preferences、プライバシー保護のために選好する条件）を問い合わせる手段と、該顧客を同定するための顧客に固有のプロキシ（customer unique proxy、以下、顧客固有プロキシという）を該データウェアハウスに格納する手段と、該プロキシを含むプライバシーカードを該顧客に発行する手段とを含むことを特徴とする装置に実現される。

6

【００１３】第三の局面から見ると本発明は、コンピュータで読み取り可能なプログラム格納装置であって、データウェアハウスに格納されているデータの収集および配布を制御するための方法を実行するための、該コンピュータにより実行可能な一つ以上の命令を具備している、プログラム格納装置に実現される。その方法は、消費者からプライバシーカードを受け取るステップと、該消費者に消費者情報およびプライバシープレファレンスを問い合わせるステップと、該顧客を同定する顧客固有プロキシを該データウェアハウスに格納するステップと、該プロキシを含むプライバシーカードを該顧客に発行するステップとを含む特徴を有する。

【００１４】本発明の一実施例は、すべてのデータ、ユーザー、およびプライバシーエレメントを含むデータとして登録されたデータの使用を統括し（administer）記録する（record）プライバシーメタデータシステム（privacy metadata system）をも利用する。このメタデータを利用するサービス機能（metadata service、以下、メタデータサービス機能という）はウェアハウスメタデータの所在を突き止め、管理し、統合し、ナビゲートすることを可能にする。メタデータサービス機能はまた一つの領域を用意し、その領域に基づいてプライバシーのすべてのシステム的局面を監査可能なフォーマット（auditable format）で登録し、統括し、ログ記録を取ることを可能にする。

【００１５】

【実施例】添付の図面のみを参照しつつ実施例を通して本発明を以下に説明する。

【００１６】図１はデータウェアハウス化システム１００の概観を表すシステムブロック図である。本システムは、中に一つ以上の拡張データベース（extended databases）１０６を格納するデータベース管理システム（database management system）１０４をもつ、保安データウェアハウス（secure data warehouse）１０２を含む。

【００１７】データベースの一つの重要な能力は、仮想的な表（virtual table）を定義し、その定義をデータベース内にユーザーが定義した名称（ユーザー定義名称）と共にメタデータとして保存する能力である。このオペレーションにより形成されるオブジェクトはビュー（view）あるいはデータベースビュー（data view）として認識される。（以下、本発明で使用される特定のデータビューを「データビュー」と呼ぶ。）データビューは仮想的な表であるから、それが必要とされるまではデータベース内のどこにも物理的に顕在化されない。データへのすべてのアクセスは（管理上の目的で行われるデータアクセスは例外として）、データビューを介して達成される。種々のプライバシー規則（privacy rules、プライバシーを保護するための規則）を与えるため、一

揃いの複数データビュー（以下、スイート（suite）という）が設けられる。プライバシーデータビューについてのメタデータ（データビュー名称、データビュー列の名称およびデータ型、並びに行を導出する方法を含む）はデータベースメタデータ内に持続的に格納される。しかしビューにより表される実際のデータはその導出された表と関連づけて物理的にどこにも格納されない。その代わり、データ自体が持続的なベース表（basetable）内に格納され、そのビューの行はそのベース表から導出される。データビューは仮想的な表であるが、ベース表に対してオペレーションを実行することができるのとまったく同様に、データビューに対してオペレーションを実行することができる。

【００１８】保安データウェアハウス（secure data warehouse）１０２はさらに、拡張データベース１０６内のすべてのデータを表すプライバシー メタデータ データビュー（privacy metadata dataviews）１０８スイートを含む。データベース１０６内のデータはこのスイートのデータビューを通してのみ、閲覧、処理、変更をすることができる。拡張データベースおよびデータビューの方式および論理モデルをさらに詳しく図２との関連で述べる。

【００１９】拡張データベース１０６内に格納されているデータへの実質上すべてのアクセスはデータビュースイート１０８を介してのみ与えられる。したがって、ビジネスアプリケーション１１０およびサードパーティアプリケーション１１２は、与えられたデータベースビューにより許可されるデータのみにアクセスできる。一実施例では、消費者のプライバシープレファランス（preferences、好ましいものとして選択された事項）を無効にしうる方策が与えられる。しかし、そのような環境では、無効の原因がデータベースに記載され、それを監査モジュール（audit module）１１８が取り出すことができる。したがって無効化が内密に起きることはできない。さらに、無効化はプライバシーメタデータ監視拡張機能（privacy metadata monitoring extensions、以下ＰＭＤＳ拡張機能または単にメタデータ監視拡張機能という）１１４によって監視することができ、無効化が起きるときは消費者に警告を与える。

【００２０】データベースへのアクセスは、プライバシーデータビュースイート１０８により次の三つの目的の場合に制限して与えられる：（１）個人データを匿名にするを可能にするためのプライバシー規則を用意すること、（２）適用除外選択をした列へのアクセスを制限すること（これはすべての個人データ、別の範疇の個人データおよび個人データ列に適用しうる）、および（３）顧客の適用除外選択に基づいて適用除外選択のために全行（顧客レコード）を削除すること（これによって、取り扱い中の顧客に対して何らかの有効な適用除外選択フラッグが設定されている行を削除し、したがってこれによっていかなる直接販売もサードパーティへの公開も阻止する）。

【００２１】データビュー１０８と通信するクライアントインターフェースモジュール１２２を使用して、クライアント１２４はクライアント１２４から収集されたデータにアクセスし、制御し、管理することができる。このデータの制御および管理は、（適当なブラウザプラグイン１２８、モデム１３０、音声による電話通信機１３２あるいはキオスク１３４、ＰＯＳにあるその他のデバイスを介する）インターネット１２６を含む広範囲の通信媒体１４０を使用して、達成することができる。そのような通信を助けるため、キオスクやＰＯＳ（販売点）にあるその他のデバイスはスマートカード１３６あるいは愛顧者カード１３８を発行することができる。キオスク／ＰＯＳ装置１３４はプライバシープレファレンスに関する消費者入力を受信し、これらのプレファレンス値に関する情報を格納したスマートカード１３６あるいは愛顧者カード１３８を発行することができる。同様にして、キオスク／ＰＯＳ１３４、スマートカード１３６、あるいは愛顧者カード１３８を使用して、消費者は必要に応じてプレファレンス値を更新し、あるいは変更することができる。愛顧者カード１３８が単純な読取り専用装置（キー リングに装着されたバーコード装置等）である場合は、キオスク１３４は必要に応じて情報を更新した取り替えカードを発行することができる。愛顧者カード１３８あるいはスマートカード１３６を使用する取引は選択的に暗号化し、匿名にすることができる。いずれのカードも選択した保安規則を与えるべく、直接にあるいはプラグインを介してサーバと対話することができる。

【００２２】このインターフェースを介して消費者はデータシェアリング（data sharing）および保持（retention）のプレファレンスを指定することができる。これらのプレファレンスにはデータ保持プレファレンスおよびデータシェアリングプレファレンスが含まれる。これらのプレファレンスによって、消費者はいついかなる状況の下で個人情報を保持し、または共有しあるいは他人に販売しうるかを指定することができる。例えば、当該消費者はそのようなデータを愛顧者カードプログラムの一部として保持することができ、あるいはそのデータの使用を特定の使用に限定することができる。さらに、消費者はいかなる状況の下でそのデータが即時販売され、統計的解析の目的に使用され、あるいはサードパーティの選択的マーケティングプログラムの目的に使用されうるかを指定できる。

【００２３】データデータウェアハウス化システム１００はまた、プライバシーサービス１５０を介してクライアントと保安データウェアハウス１０２との間の匿名通信を可能にする。ユーザーが匿名の取引を望むときは取引はプライバシーサービス１５０へ送信される。プライ

バシーサービス１５０はプライバシー規則データベース１５２および他の保安情報１５４にアクセスし、プライバシー規則および保安情報を使用して消費者の身元を決定できるすべての情報を除去（浄化）する。浄化された取引情報は次いで保安データウェアハウス内の匿名保護インターフェースモジュール１６０へ回送される。保安データウェアハウス１０２との通信はプロキシユーザー同定手順を使用する。この同定はプライバシーサービス１５０により消費者の使用者名または他の同定情報から生成される。もしも顧客が匿名取引を必要としないなら、取引は、拡張データベース内に取引情報を格納できる小売業者に直接に提供される。

【００２４】データビュースイート１０８は単独に拡張データベース内のデータへのアクセスを与えるので、データビュースイート１０８もまた保安データウェアハウス１０２の保安を監査するための便利かつ合理的手段を与える。

【００２５】保安データウェアハウス１０２もまたメタデータ監視拡張機能１１４を含む。このメタデータ監視拡張機能１１４によって顧客は個人データの使用を監視するための規則を発生させることができ、またメタデータ定義の変更が生じたときは警告１１６または取り消しを送信することができる。顧客の個人情報が拡張データベース１０６から読み取られるとき、または拡張データベース１０６に書込みがなされるとき、拡張データベース１０６に格納されている適用除外選択デリミタ（opt-out delimiters）が変更されとき、あるいは表またはデータビューがアクセスされるときに、消費者はメタデータ監視拡張機能１１４を制御して警告を発生させることができる。この代わりに、顧客が後でアクセスできるよう、発生した警告を記録しておくことができる。

【００２６】メタデータ監視拡張機能１１４はまたデータソース情報を記録するので、顧客は保安データウェアハウス１０２に格納されているデータのソースを決定することができる。データソースは顧客であるかも知れないし、あるいはサードパーティを媒介とするソースであるかも知れない。本発明のこの特徴は、顧客が誤った情報を訂正したいときのみならず、当該誤りが同じデータベースもしくは他のデータベースで繰り返されることがないよう、誤った情報ソースを特定したいとき、特に有用である。

【００２７】またデータのソースを直接に表データから確かめることができるよう、ソースデータはデータ表の各列にあるいは一組の列に格納することもできる。本実施例では、メタデータ内に情報ソースの情報をすべての顧客に対して複製することをしなくても各顧客が異なった情報ソースをもつことができるよう、ソースを同定するデータを一般化することができる。

【００２８】同様にしてメタデータ監視拡張機能１１４も、データターゲット情報を記録するので、顧客は誰が彼らの個人情報の受信者であるかを決定することができる。この特徴もまた顧客の個人情報に関して公開活動を監視する上で有用であるのみならず、複製された誤りを訂正する上で、有用である。

【００２９】メタデータ監視拡張機能１１４はまた、プライバシーデータビュースイート１０８への変更のみならず拡張データベース１０６からの読み取りおよびそれへの書き込みを追跡することにより、監視機能のサポートに使用することができる。

【００３０】本発明は、プロセッサおよびランダムアクセスメモリ（ＲＡＭ）のようなメモリを含むコンピューターに実現することができる。そのようなコンピューターは普通、ディスプレイと動作上結合しうる。ディスプレイは、ユーザー向けウィンドウのようなイメージをグラフィックユーザーインターフェース上に呈示する。コンピューターはキーボード、マウス装置、プリンタ等の他の装置に結合することができる。もちろん、当業者は上記のコンポーネントの任意の組合せあるいは任意数の異種コンポーネント、周辺機器その他の装置をコンピューターに使用することができることを認識できよう。

【００３１】一般に、コンピューターはメモリ内に格納されているオペレーティングシステム、およびユーザーインターフェースの制御の下に動作する。ユーザーインターフェースは入力およびコマンドを受信すると共にグラフィックユーザーインターフェース（ＧＵＩ）モジュールを介して結果を呈示する。ＧＵＩモジュールは普通、別個のモジュールであるが、ＧＵＩ機能を実行する命令はオペレーティングシステムまたはアプリケーションプログラム内に常駐させ、分布させ、あるいは特別の目的のメモリおよびプロセッサを使って用意することができる。コンピューターはまた、ＣＯＢＯＬ、Ｃ++、ＦＯＲＴＲＡＮその他のプログラム言語で書かれたアプリケーションプログラムがプロセッサで読み取りできるコードに翻訳しうるコンパイラをもつことができる。翻訳完了後、アプリケーションは、コンパイラを使って発生された諸関係式および論理を使用してコンピューターメモリ内に格納されているデータにアクセスし、操作する。

【００３２】本実施例では、オペレーティングシステムをなす諸々の命令、コンピュータープログラムおよびコンパイラはコンピューターが読み取り可能な媒体、すなわちデータ格納装置１７０内に実体的に実現される。この格納装置１７０はジップドライブ、フロッピーディスク、ハードウェアドライブ，ＣＤ－ＲＯＭドライブ、テープドライブ等の一つ以上の固定式もしくは着脱式データ格納装置でよい。さらに、オペレーティングシステムおよびコンピュータープログラムは諸々の命令からなるが、これらの命令は、コンピューターにより読み取られて実行されると本発明を実現およびまたは使用するのに必要な諸ステップをコンピューターに行わせるものであ

る。コンピュータープログラムおよびまたは諸々の命令もメモリおよびまたはデータ通信デバイス内に実体的に実現することができ、それにより本発明に基づくコンピュータープログラム製品あるいは製造物品を作製することができる。上記のとおりであるから、「プログラム格納装置」、「製造物品」および「コンピュータープログラム製品」と言う用語はここではコンピューターにより読み取り可能な任意の装置、あるいは媒体からアクセス可能なコンピュータープログラムを含む。

【００３３】当業者は、本発明の範囲から逸脱することなくこの形態に任意の改変を加えることができることを認識されたい。例えば当業者は上記のコンポーネントの任意の組合せ、あるいは任意数の異なるコンポーネント、周辺機器その他の装置を本発明に使用することができることを認識されたい。

【００３４】論理モデル

図２は保安データウェアハウス１０２およびデータビュースイート１０８の論理モデル例をより詳細に示す図である。拡張データベース１０６は表２０２を含んでおり、この表は次の三つの部分：同定情報部分２０４、個人情報部分２０６、および機密情報部分２０８に分割される。個人情報部分２０６はデータ列２２０、２３２、２４４、および２４６を含み、これらの列は消費者の身元を表す情報を格納する。これらの列には消費者口座番号列２２０、氏名列２３２、住所列２４４、および電話番号列２４６が含まれる。顧客表２０２の同定部分２０４も一つ以上のデータ制御列２１２を含んでおり、これらの列はプライバシープレファレンスすなわち表中の関連データに対する「適用除外選択」を反映するデータを特定している。ここに例示した実施例では、列２２２－２３０は一つ以上の文字（［A］または［D］）すなわち当該顧客のデータレコードに対するプライバシープレファレンスを指定するフラッグ（［1］および［0］で表されている）を格納する。ここに開示する実施例ではこれらのプライバシープレファレンスは次の事項に対する「適用除外選択」を含む：（１）直接販売、（２）当該顧客を同定する情報および個人データの公開、（３）匿名による個人データの公開、（４）自動マーケティングの判定を行うための個人データの公開、および（５）機密データの公開と使用。表２０２はまた、グローバルデータ制御列２１０を含む。この列は顧客が最大限のプライバシーを望むことを示すのに使用することができる。

【００３５】ここに例示する実施例では、「ビル　Ｋジョーンズという名前の顧客がグローバルデータ制御列２１０に「0」を選択することにより、ある程度のデータ収集、解析、あるいは流布を許可している。彼はさらに、彼の身元情報と共にあるいは匿名で、彼の消費者情報を直接販売に使用することができること、およびサードパーティに公開できることを示している。彼は自動処理を行うのにデータを使用することを許可しているので、機密データを流布することを許可するであろう。

【００３６】一実施例では前述の論理モデルを実現するのにテラデータ（TERADATA）データベース管理システムが使用される。これを使用することにはいくつかの利点があある。

【００３７】第一に大量のデータを格納し取り扱えるテラデータの能力が多数のいろいろのビューの構築を容易にするとともに、保安データウェアハウス化システム１００が論理データモデルを第三の正規の形態でもしくは正規の形態に近い形で利用することを可能にする。

【００３８】第二に、データビューサブセットまでデータを狭めるための一連の選択としてＳＱＬ照会（SQL queries）を実行するシステムとは異なって、本テラデータデータベース管理システムは適当なベース表から直接に必要な列を選択するＳＱＬを発生すべくデータビューベース（dataview base）の照会を書き直す。他のビューはデータをビューサブセットにまで狭める前に表全体を作成するが、テラデータは適当な列および行を結果表（処理結果をまとめた表）中に選択的に引き抜くＳＱＬを発生する。この方法は、前述の論理モデルを実現するのに特に有利である。

【００３９】第三に前述の論理モデルは一般に複雑な照会および広範なＳＱＬステートメントを含むデータビューを生ずる。テラデータデータベース管理システムは、そのような照会およびＳＱＬステートメントを最適化するのに特に有効である。

【００４０】上に教示したことを使用して、特別な個々のプライバシー条件に合うよう、かつ各データベースアプリケーションを制御するのに必要な条件に合うよう、代わりの定義データ制御列構造を有する代わりの論理モデルを実現することができる。

【００４１】データビュー

データビュースイート１０８には多数のデータビューが用意されている。これらのデータビューには標準ビュー２６０、特権ビュー（priviledged view）２６２、匿名ビュー（anonumizing view）２６４、および適用除外選択ビュー２６６が含まれる。これらのビューはデータ制御列２１２に置かれている値に基づいて顧客表２０２内のデータへの可視度（visibility）を制限する。

【００４２】標準ビュー２６０は、列２２４内のフラッグ（個人情報および同定情報が流布できることを意味する）あるいは列２２６（個人情報が匿名でのみ流布し得ることを示す）のいずれかがアクティブ化されない限り、個人データを呈示しない。したがって、標準ビュー２６０は消費者が適当なフラッグを適当な値に設定しない限り、個人データを選択的にビューから隠す。

【００４３】スケーラブルデータウェアハウス（scalable data warehouse, SDW）の顧客データベース統括者（customer database adoministrators）は、ルーチン

ユーザーに対しては個人情報のすべての列が隠されるように、顧客表（顧客に関する個人情報を含む任意の表）中に入るビューを設定する。これにより、すべてのルーチン決定サポート（routine decision support、DSS）アプリケーションおよびウェアハウスデータへの照会アクセスを備えたツールを個人情報の閲覧から適用除外することができ、その結果これらのアプリケーションおよびツールのすべてのエンドユーザーも同様に個人情報の閲覧から適用除外される。

【００４４】既存のＳＤＷ顧客に対して混乱が生じることを最小限に留めるため、プライバシーデータにアクセスする既存のすべてのアプリケーション内のベース表に使用されるものと同一の氏名を使用してデータビューが設立され、その氏名に対応するベース表の氏名が他の値に命名し直すことができる。こうして、既存アプリケーションが（ここではデータビュー経由で）私的データへアクセスしようと試みても、その私的データはユーザーがもつ特権に応じてデータビューによりふるい落とされる。このアプローチを使用すれば既存のアプリケーションを改変する必要はまったくない。その代わり、論理データモデルおよびデータベースの方式が改変され、更なる命名規約が導入される。

【００４５】特権ビュー２６２は、データベースの管理およびまたは維持（例えば新規顧客の挿入、前顧客の削除、住所変更など）に必要とされる特権的（クラス「Ａ」の）アプリケーション１１０Ｂに対してのみ、およびプライバシー関連機能（顧客について収集された個人情報を顧客に通知すること、個人情報を変更／更新すること、および「適用選択／適用除外選択」制御を適用することなど）の関連機能）を取り扱うアプリケーションに対してのみ、提供される。例えば、顧客プライバシープレファレンスを閲覧し、指定し、変更するのに使われるクライアントインターフェースモジュール１２２は、特権アプリケーションである。特権アプリケーションが特権アプリケーションであると適切に同定されることを確実ならしめると共に、特権ビュー２６２が承認されていない任意の主体によるアクセスを防止するため、適当な保安対策がとられる。

【００４６】ある種のＳＤＷアプリケーション（「クラスＢ」）は顧客の振る舞いの見通しを得るため、例えば顧客の傾向あるいは行動パターンを同定するため、個人データに解析を施すことができる。そのようなアプリケーションは（知的業務者あるいは「パワーアナリスト」と呼ばれる）エンドユーザーが駆動することができる。かかるエンドユーザーとは即興的に照会を行うことができるエンドユーザー、典型的にはカスタム構築したソフトウェアあるいは標準的照会もしくはＯＬＡＰツールを使って、上記のパターンを発見するようなエンドユーザーである。彼らエンドユーザーは発掘ツール（data mining tools）も使用することができる。このツールでは統計的もしくは機械学習アルゴリズム（machine learning algorithms）が当該アナリストと共にパターンを発見し、そのパターンからアナリストが予測モデルを構築する。

【００４７】最も有効な値を導出するため、解析アプリケーションは利用可能なすべての形態の個人情報にアクセスしなければならない。必要とされる個人のプライバシーを尊重すると同時にそのようなアクセスを可能にするため、特別の「匿名化」データビューが使用される。これらデータビューは個人データフィールドへのアクセスを提供するように設計されているが、データ所有者を同定できる情報（例えば氏名、住所、電話番号、社会保障番号、口座番号など）を含むすべてのフィールドを遮蔽するように設計されている。

【００４８】匿名化ビュー２６４は個人情報の閲覧および解析を許すが、列２２４内のフラッグ（当該消費者を同定する情報と個人データの公開を許可するフラッグ）が選択されていない限り、同定情報部分２０４に格納されている情報を閲覧および解析から遮蔽する。このデータは解析アプリケーション１１０Ｃに提供することができる。このアプリケーションはデータ発掘および即興的照会を許容する。消費者が許可するなら、この情報はまたサードパーティアプリケーション１１２にも与えることができる。

【００４９】別のクラスの特権アプリケーション（「クラスＣ」）にはある形態の処置（action）を行うために個人情報を使用するアプリケーション、たとえばマーケティングアプリケーション（郵便もしくは電話による勧誘を行うものなど）が含まれる。これらのマーケティングアプリケーションは各顧客に対して設定された「適用選択／適用除外選択」制御を受け、アクティブ化された「適用除外選択」指標（indicator）をもつすべての記録を除去しあるいは隠す特別のデータビューを介して、顧客情報にアクセスする。したがって、例えばマーケティング勧誘を受信しない選択をした任意の顧客は、マーケティングアプリケーションが生成する任意の接触リストから適用除外される。

【００５０】「適用除外選択」指標はデータビュー経由で顧客表に追加され、あるいは既存の顧客表に接合される新規の列である。（これは論理データモデルに追加される変更である。）一実施例では、各顧客行に対するこの列の値は、初めは「適用除外選択」に設定される（あるいは法律で許可されるなら「適用選択」に設定される）が、クライアントインターフェースモジュール１２２経由で改変することができる。このモジュール１２２はプライバシー制御に関する顧客のリクエストを処理する。

【００５１】多重「適用除外選択」指標は、各顧客レコードに対して設定することができる。最小限、「直接販売」、「身元データのサードパーティへの公開」、「サ

15

ードパーティへの匿名データの公開」、「自動判定」、および「機密データの使用」に対する５個の適用除外選択が用意される。しかし、さらに詳細な顧客のプレファランスに基づいてさらに詳細に分類した適用除外選択を設計することができよう。例えば、「直接販売」に対する適用除外選択項目は、電話、ダイレクトメール、および電子メールによる接触、および「その他」の処置のための雑類事項に分けることができよう。こうすると８個の別個の適用除外選択が生じる。

【００５２】適用除外選択ビュー２６６は処置アプリケーション１１０Ｄによって自動判定（automated decisions）を行うために情報を利用することは許可する。そのようなアプリケーションはたとえば電話あるいは郵便による勧誘などの処置を行うものである。この情報の閲覧は列２２８内のフラッグにより制御される。列２２８に格納されている値は、この代わりとして十分な値域をもつ一文字を含むことができる。その文字は、当該勧誘が許可されることを定義するに留まらずいかなる種類および範囲の勧誘が許可されるかを指示することを許容できる。

【００５３】（マーケティングや解析等を目的として）サードパーティに個人データを公開しあるいは照会するアプリケーションはクラスＣ（「適用除外選択」）のビューおよびクラスＢ（「匿名」）のビューの両方を受ける。もしも顧客が、サードパーティによる自分のデータの使用を適用除外とする選択をしていると、「適用除外選択」データビューが適用され、それらの行（レコード）は出力から適用除外される。他の顧客は彼らのデータが匿名であることを条件にサードパーティへの公開を「適用選択」しているかも知れない。そのような場合には顧客データは出力される前に「匿名化」データビューを介して匿名化される。他のすべての場合は顧客は身元が同定できる形式で自分の個人データが公開されることの適用選択をしている。この場合は個人データが身元同定データと共に出力される。

【００５４】適用選択もしくは適用除外選択をするためのさらに細かい分類を用意することができる。種々の許可および保護に関して顧客毎に同意を求め、特定の適用選択もしくは適用除外選択を設定できる。例えば、サードパーティへの公開は、個人の特徴および個人の身元の両方に関連する特定のデータに基づいて行うことができる。顧客は自分の住所および関心事のプロファイルを提供することに同意するが、経済情報および電話番号については同意しないこともあり得る。

【００５５】適用選択／適用除外選択は各顧客のさらに詳細なプロファイルおよび関心事が得られるようにさらに拡張することができる。例えば、適用除外選択（例えば第４節で同定した８個の適用除外選択）のクラスをそれぞれ別個に各範疇の個人データ（例えば人口統計学的データ、プレファレンスデータなど）に適用することができよう、あるいは個人データの各特定データ項目（例えば年齢、性別、ハイキング趣味、好みの靴ブランドなど）にまで適用することができよう。このようにして、顧客はいくつかの関心領域に関連するいくつかの処置を適用除外選択することができ、他の項目を適用選択する（例えばランニングシューズについてダイレクトメールの受信を適用する）ことができる。

16

【００５６】図３はさらに細かく分類された適用選択および適用除外選択を備えた保安データウェアハウス１０２の、別の論理モデルを示す。この実施例では、各クラスのプライバシープレファレンスが各範疇のデータ（例えば人口統計など）に別個に適用され、あるいは個人データ（例えば年齢、性別、ハイキングの趣味、あるいは好みの靴ブランド）の各特定データ項目にまで適用される。例えば、消費者ビル・Ｋ・ジョーンズはいくつかの目的には彼の氏名へのアクセス許可するが、その他の目的にはアクセス不可とする選択をなしうる。これらの制限は列３０２-３１０の記入事項として適切な組合せのフラッグを入力することにより選択することができる。同様にしてジョーンズ氏の名前の格納およびまたは使用に関してプライバシープレファレンスを指定するのに列３１２-３２０を使用することができる。列３１２-３２０に定義されたプレファレンスは、列３０２-３１０に記述されたものと異なるかも知れないし、同一かも知れない。本発明はまた、さらに詳細な顧客のプレファレンスに基づいて、前述の保安プレファレンス範例（secure preference paradigm）を細密な多重的プレファレンス（multiple fine-grain preferences）へ拡張することを可能にする。例えば、直接販売は電話、ダイレクトメール、電子メール、および「その他」の処置をとりたいキャッチコールに対する別々のプライバシープレファレンスに分解することができよう。さらに、直接販売の範囲を一回の接触だけを許可するように指定することができよう。

【００５７】別の実施例ではデータ暗号を使用することによって、拡張データベース１０６およびデータビュースイート１０８が果たす特徴的な保安およびプライバシー保護がさらに強化される。これは与えられた行のデータを暗号化コードで暗号化することにより、あるいは各データフィールドに固有の暗号化数を与えることにより、行うことができる。その代わりとして、消費者のプライバシープレファレンスを実行することができるようにいろいろの階層的レベルでデータを暗号化することもできる。

【００５８】一実施例では暗号化技術は任意の同定フィールド上で使用されると共に行単位でも選択的に適用される。この技術によれば、顧客が（例えばデータを発掘する目的などで）匿名のままに留まることを可能にする一方、データ暗号化権を有するアプリケーションもしくはデータ請求者に対しては積極的に身元の同定を受け入

れることが可能になろう。

【００５９】データビューのオペレーション

本発明のデータビュースイート１０８におけるデータビューは、ベース表の適当な列および行を結果表中に選択的に引き入れるＳＱＬステートメントを発生する。（データをビューサブセットにまで狭める前に表全体を作成する）従来技術と比較して、本技術はデータ請求者にデータを呈示するのために必要な処理を低減する。

【００６０】データベース所有者すなわちＢＢＢ ＯＮＬＩＮＥ、ＴＲＵＳＴＥ、ＰＲＩＣＥ－ＷＡＴＥＲＨＯＵＳＥ、ＴＲＷ、ＤＭＡあるいはＣＰＡ ＷＥＢＴＲＵＳＴ、あるいはＮＣＲのような独立の監査サービスは、定期的にもしくは苦情を受けたときに、安価にデータベースの見直し（review）を行うことができる。これらの見直しでは論理データモデルとデータベースのスキーム、当該システムを使用するアプリケーションとユーザー、およびテラデータアクセスログが調査される。

【００６１】論理データモデルの見直しでは、データビュー構造を調査し、（個人情報へのアクセスを制限している）正規ユーザー用の「標準」ビュー、解析アプリケーション用の「匿名」ビュー、およびその他のアプリケーション用の「適用除外選択」ビューの存在が調査される。

【００６２】これらのアプリケーションの見直しおよびユーザーの見直しは、アプリケーション、ユーザー、およびそれらに付与されているアクセス権を調査する。この見直しは、「クラスＡ」特権をもつアプリケーション／ユーザーが「個人データ」データビューへのアクセス権をもっていること、「クラスＢ」解析アプリケーション／ユーザーが「匿名化」データビューへのアクセス権をもっていること、「クラスＣ」処置アプリケーション／ユーザーが「適用除外選択」ビューへのアクセス権をもっていること、個人データの出力表あるいはファイルを生成するアプリケーションが「適用除外選択」および「匿名化」ビューへのアクセス権をもっていること、並びに他のアプリケーションが「標準」ビューを使用することの確認を行う。

【００６３】最後に、テラデータアクセスログあるいは別のデータベース管理システムから得た類似のログが見直される。これは行われたアクセス活動が当該データソースにより規定されているプライバシーパラメーターに適合していることを確証するためである。

【００６４】図４は本発明の特徴であるプライバシー監査オペレーションの概観を表す図である。データ請求主体が拡張データベース１０６内のデータへのアクセスを望むときはいつでも、リクエストはデータベース管理システムインターフェース１０９に対してなされ、インターフェース１０９がプライバシーパラメーターにしたがって当該データベース表内のデータへのアクセスを制御する。当該リクエスト主体のステータスに基づいてデータビュースイート１０８からリクエスト主体に与えられるデータビューを使って、拡張データベース１０６の表がアクセスされ、そのデータが提供される。同時に、データベースアクセス（アクセスが不成功であるときはその試みられたアクセス）がアクセスログ（access log）４０２に記録される。アクセスログ４０２は、アクセスもしくはアクセスの試みの形態、アクセスを生じたリクエストのテキスト（ＳＱＬ）、アクセスの頻度、リクエストされた処置、リクエスト主体またはアプリケーション名または識別データ、および参照されたオブジェクト（表、データビューおよびまたはマクロ）に関する情報を含む。アクセスログ４０２により、データビュースイート１０８内のデータビュー、マクロスイート１１１内のマクロ、あるいはデータベース１０６内のベース表へのすべてのアクセスを監査することができる。アクセス特権を付与しまたは呼び出す総ての活動が同様に監査できる。これが可能であるのは、アクセスログ４０２の内容と表／データビュー／マクロの定義とからプライバシー規則が施行されているかあるいは破られているか決定ができるからである。

【００６５】プライバシー監査モジュール１１８が設けらるのは、プライバシーパラメーターを有効に適用すべくアクセスログ４０２内のデータについてプライバシー解析を行うためである。プライバシー監査モジュール１１８はプライバシーに関するすべてのイベント（event）を追跡し、個人データへのアクセスに関する活動を要約し、プライバシー規則のいかなる疑惑ある違反にもフラッグを立てる。プライバシーテストスイート４０４は、プライバシー規則を「破る」ことを試みてからアクセスログ４０２を調査してプライバシー規則が適用されたかあるいは破られたかを決定するプログラムその他の手順を含んでいる。プライバシー監査モジュール１１８はこれを、顧客プライバシープレファレンスが適用されているか否かを独立に評価するサービス監査者またはデータウェアハウスマネージャが使用できるように、手直しできる。

【００６６】メタデータサービス

メタデータサービスはプライバシーメタデータサブシステム（privacy metadata subsystem、PMDS）拡張機能１１４を含む。ＰＭＤＳ拡張機能１１４は多数のパラメーターを格納し、追跡するとともにこれらのパラメーターを使ってプライバシーが関わる活動を追跡する。追跡されたパラメーターには、（１）システムに現在あるすべてのデータエレメント（データベース、ユーザー、表、ビューおよびマクロを含む）のデータ復号化、（２）システムに対してソースとなった内部エレメントのデータ復号化、（３）システムに対してソースとなった外部エレメントのデータ復号化、（４）システムにとってターゲットとなった内部エレメントのデータ復号化、（５）システムからエキスポートされたデータエレメントのデ

ータ復号化、（６）すべてのユーザー、グループおよびアプリケーション並びに当該データへのそれらのアクセス権のプロファイル、（７）データのアクセス／更新、表／ビュー／マクロの生成、特権の付与／取消し、ユーザープロファイルの変更、およびトリガーに関するイベント記録を含む。

【００６７】ＰＭＤＳ拡張機能１１４はまた、プライバシーに固執するデータコントローラを支配する実行可能なビジネス規則と、テラデータログ（例えば記録の開始／終了）の操作（manipulations）に関するイベントの記録もしくは別のデータベース管理システムにおけるそれと類似の記録に関するイベントの記録とを格納し管理する。

【００６８】また、ＰＭＤＳ拡張機能１１４はプライバシーが関わるメタデータを見直し、管理するための高レベルＧＵＩ４０６をプライバシー統括者に提供する。このＧＵＩは、すべての顧客（消費者またはデータの主体）の情報に対するデータベースとそれらの表／ビューマクロ構造のグラフィック表示、および関連するユーザー／ユーザーグループの特権のグラフィック表示を含む。またＧＵＩ４０６は、プライバシー統括者がＧＵＩ４０６を介して与える定義に基づき、プライバシー規則を設定すると共にその設定の結果、データビュー、マクロ、もしくはアクセス権を発生するパラメーター駆動手段（parameter-driven means）を提供する。またＧＵＩ４０６は、外部監査者が当該サイトのプライバシー保護策の見直しを行う際に彼を案内する便宜を提供する。

【００６９】ＰＭＤＳ拡張機能１１４はまた、報告を行う便宜的機能を提供する。これは種々のデータベースおよびＰＭＤＳログの内容を解析してプライバシー関連の活動に関して報告を行うものである。プライバシー統括者はそのようなプライバシー報告を対話形インターフェースもしくは印刷された報告を介して見直すことができる。独立の監査者はプライバシー統括者と共に、そのような報告の助けを借りて監査を行うことができる。

【００７０】またＰＭＤＳ拡張機能１１４は、消費者の個人データおよびそれに関連するプライバシー規則へのアクセス、それらの見直し、および訂正を行う消費者をサポートするためのＧＵＩアプリケーション／ユーティリティを別途提供する。またＰＭＤＳ拡張機能１１４は、プライバシー関連のイベントに関するさらに詳細な記録をとるための便宜を提供することもできる。

【００７１】マクロ

単独であるいはここに記載するデータビューと組み合わせてマクロ１１１（すなわちデータベース管理システムインターフェースに格納された手順）を使用してデータの制御とデータへのアクセスを記録することができる。データプライバシーパラメーターを適用すべくマクロを使用する場合は、ユーザーは「選択」アクセス権を与えられない。その代わり、ユーザーは、マクロスイート１１１内のマクロへのアクセス権を与えられる。このマクロは実際のデータアクセスを行うと共に将来の監査を目的としてアクセスログ４０２内のイベントを記録する。その場合も、これらのマクロは適用除外選択された行および列へのアクセスを制限する前記ビューを通して当該データに対し実行される。そのようなマクロは単一行アクセスを記録するのに特に適している。

【００７２】データ辞典

データ辞典４０８は、システム内のすべての表、データビュー、およびマクロ、システム内のすべてのマクロ、すべてのユーザーおよび彼らの特権（ユーザーが所有しているマクロに関する特権を含む）を含めたデータベーススキーマに関する情報を格納している。

【００７３】プロセス

図５は本発明の一実施例を実施するのに使用するオペレーション例を示す流れ図である。このプロセスは愛顧者カード１３８あるいはスマートカード１３６のような消費者プライバシーカードを求めるリクエストを顧客から受け取ることにより始まる。これは、モデム１３０を介して行われるインターネット１２６，電話１３２，あるいはキオスクもしくはＡＴＭ１３４経由で達成することができる。これはブロック５０２に例示してある。次に消費者は、（氏名、住所、および電話番号等の）消費者個人情報および上述した消費者のプライバシープレファレンスを得るための問い合わせを受ける（ステップ５０４）。消費者は次いで要求された情報を入力する。次にその顧客を同定する顧客固有プロキシが発生され、顧客の個人情報と関連づけられ、データウェアハウス１０２に格納される。これはブロック５０６に示してある。次に顧客のプライバシープレファレンスを明示するプライバシーカードが顧客に発行される（ステップ５０８）。このプライバシーカードはメモリと限定的な処理機能およびＩ／Ｏ機能の付いたスマートカードでもよく、あるいはバーコード付きのカードでもよい。

【００７４】図６は顧客を同定する顧客固有プロキシをデータウェアハウスに格納するために実行するオペレーション例を示す流れ図である。最初に、ブロック６０２に示すようにプロキシが発生される。

【００７５】次に、ブロック６０４および６０５に示すように、この発生されたプロキシがデータウェアハウス１０２およびプライバシーカードに格納される。

【００７６】図７は、プライバシーカードがバーコードのような読み取り専用機能を備えた単純な愛顧者カードであるときに顧客を同定する顧客固有プロキシをデータウェアハウスに格納するために実行されるオペレーション例を示す流れ図である。この実施例では、カード（すなわちカード上のバーコード）から予め格納してあるプロキシが読み取られ、データウェアハウスへ送信され、データウェアハウスに格納される。これはそれぞれブロック７０２および７０４に例示してある。この代わり

に、バーコードまたはプロキシを示す他の表示はキオスクもしくはＡＴＭ１３４で、あるいは顧客のコンピュータに接続されているプリンタで印刷することができる。

【００７７】図８はプライバシーカードを使用する商取引に関与する際に実行されるオペレーション例を示す流れ図である。最初に、ブロック８０２に示すように、顧客の固有プロキシを含む取引リクエストが消費者から受信される。消費者は取引を完了すると、ブロック８０４に示すように取引に関するデータがプロキシに関連づけられる。次に、ブロック８０６に示すように、この取引データはプロキシとの関連が維持されるよう、データウェアハウス１０２に格納される。

【００７８】図９は消費者のプライバシープレファレンスを管理するためにプライバシーカードを使用するときに実行されるオペレーション例を示す流れ図である。最初に、データウェアハウス内のプライバシープレファレンスを管理するためのリクエストが消費者から受信され、受理される（ステップ９０２）。このリクエストは消費者のプロキシを含んでおり、通常、保安のため暗号化されている。顧客の身元が照合確認された後（ステップ９０４）、顧客はデータベースウェアハウスに格納されているプライバシープレファレンスを閲覧、変更、ないし操作する事ができる。

【００７９】上記のオペレーションで述べたように、顧客は小売業者の施設内にあるＡＴＭ等の自動サービス式キオスク機１３４でプライバシーカードを取得する手続きをとることができる。キオスク機は消費者に種々のプライバシープレファレンスを問い合わせ、消費者の氏名、電話番号、および郵便の宛先を収集し、任意の参与機関において直ちに使用できる広域カードであって特別扱い（たとえば「高頻度購入者」の扱い）、特典、特別割引、およびボーナス点（「高頻度航空旅行者へのおまけ飛行距離点」など）に直ちにアクセスできるプライバシーカードを発行する。

【００８０】キオスク１３４と対話することにより、消費者は詳細なレベルでプライバシーをいくつかの特典と交換することができる。たとえば、消費者は、或特定の「雑種」メールあるいはカタログを所望するがそのほかのものは要らない、と表明することができる。あるいは顧客は、特定のタイプの店もしくは特定の店の家庭訪問を望むがある時間帯に限る、という意思を表明しうる。言い換えると、プライバシーカードは、いかなるデータが収集されそのデータで何が行われるかを消費者が完全に制御できるようにする。すべてのプライバシープレファレンスは、新たなプレファレンスが厳守される完全な保証を保ちつつ、消費者がいつの時点でも変更することができる。さらに、消費者は各小売業者施設がプライバシープレファレンスを守ることに信を置く必要はない。消費者は、カードを発行し消費者のプレファレンスを追跡するプライバシー保護サービス代理店のみを信託しなければならない。最後の点として、プライバシーカードは任意の参与機関で有効であるので、消費者はただ一つのカードのみを携帯すればよく、ただ一つのプライバシープレファレンスプロファイルを統括すればよい。

【００８１】上記のことから、小売業者は無用の雑多な郵便、不要の電話勧誘、商品見本等により消費者を苛立たせることなく消費者のプレファレンスに応えることが可能となる。さらに、小売業者は大量のメールや不要の電話勧誘を回避する点で費用を顕著に節減できる。最後に、小売業者は顧客のプライバシー保護の希望を踏みにじる危険を冒すことなく、彼らの最も忠節な顧客の購買パターンに関する詳細な分析を行うことができる。自動認識システムと結合すれば、小売業者は、いつ顧客が小売りアウトレットに入り、どの程度にその顧客が名前を伏せたまま挨拶されたいか、あるいは買い物の手助けを希望しているか、または呼び止められずに店内を歩きたいか否かを決定することさえできる。

【００８２】上記のシステムは、小売業者が消費者のプレファレンスを出し抜くことができない、との保証の下に消費者自身にプライバシーの責任を持たせるので、データ発掘、雑多のメール、限度を超えた電話勧誘、あるいは商品見本に対する規制もしくは法的制御がまったく必要ない。

【００８３】一実施例では、プライバシーカードはこれに或金額の金銭、或程度の計算機能、および或程度のソフトウェアを備えたスマートカードである。プライバシーカードは、小売業者の販売点（ＰＯＳ）ステーションにあるスマートカードリーダーに装着したときは、一人の顧客に固有の同定データである同定番号（id number）を発生する。これは各小売り機関ごとに異なるが、複数の来店の間のみならず同じ小売業者が所有する個々の店舗間で一貫したものである。プライバシーカードは、消費者の家庭のパソコンのスマートカードリーダー中に挿入したときも、消費者が小売業者のウェブサイトと対話しているときと同じ同定番号を発生する。プライバシー保護サービス代理店であるサードパーティーは、メールアドレス、電話番号および電子メールアドレスについてのみ、同定番号と消費者の氏名との間の翻訳ができる。したがって、小売業者は、当該消費者の購買行為を追跡することができるものの、決してその消費者が誰であるか知ることはない。消費者が自分の愛顧者カードプロファイルの一部として人口統計学的データに必要事項を記入し、小売業者がそれにアクセス可能であるとする意思があるなら、小売業者はプライバシー保護サービス機関を介してその統計データにアクセスすることができる。

【００８４】小売業者が郵便、電話あるいは電子メールを介してその消費者に接触することを希望するときは、小売業者はコンピュータプロトコル経由で当該プライバシー保護サービス機関に通報しなければならない。プラ

イバシー保護サービス機関のコンピュータはその消費者の最も最近のプライバシープロファイルを検査し、もしもその消費者がそれを許可するなら、電子メールを転送し、電話をかけ、あるいはチラシ広告を郵送する。

【００８５】別の実施例

図１０は本発明の別の実施例を示すブロック図である。この実施例では二つのデータベースを使用する。その最初のものは匿名化されたデータベース（以下、匿名データベースという）７０８で、これは匿名のデータ（以下匿名データという）および表７０６内に格納されているデータに関連づけられている変名を格納する。第二のデータベースは信託データベース（trusteddatabase）１００４で、これは変名を顧客同定情報に関連づける表１００２を格納する。この方法では、顧客の氏名は信託データベース１００４内に別個に格納される。このデータベースはデータ管理システムインターフェース１０９がこれを使用して顧客の身元を変名に、したがって匿名デバイス１００８に格納されているデータに、結びつける。この信託データベースはまた個々人のプライバシーパラメータを格納する。

【００８６】クライアントの変名はクライアントに、愛顧者カード１３８またはスマートカード１３６を発行することにより提供され、またはクライアントのコンピュータもしくはその他の手段によりインターネット１２６あるいはオンライン通信で提供される。こうすると変名は消費者取引に対するプロキシとして使用することができる（従ってこのようにして収集されたすべてのデータが匿名状態に維持される）。当該顧客の身元を確認するためのデータ発掘を防止するために望ましければ、異なる業者ごとに、あるいは異なる店舗ごとにいろいろの匿名を使用することができる。

【００８７】顧客は、データプライバシープレファレンスの選択の仕方により非匿名データの収集、使用または配布を許可する決定をすることができる。これらのプレファレンスはデータ管理システムインターフェース１０９により強行され、愛顧者カード１３８，スマートカード１３６を使用するクライアントにより提供される。一実施例ではインテリジェントソフトウェアエイジェント（intelligent software agent）がデータ発掘機能を実行して顧客のパターンを調査し、発掘結果に基づいてデータプライバシーパラメータの提案を作成する。

【００８８】もう一つの実施例では、多重レベル保安プライバシーシステムにおいて別個の信託データベース１００４および匿名データベース１００８を使用する。このシステムでは異なる法制によるプライバシー保護条件に適合し、いろいろの小売りアウトレットに適応し、またはいろいろの個人プレファレンスを許容するため、ここに開示した暗号化方法、マクロ、データビューおよびまたは別個のデータベース技術が組み合わされる。

【００８９】図１１はプライバシーデータウェアハウスの別の実施例を示す図である。前述した実施例におけると同様、データベース管理システム１０４のデータへのアクセスは、再びデータビュースイート１０８内のデータビューを介して、あるいはマクロスイート１１１内のマクロ２を介して達成される。この実施例でもまた、プライバシーサービス機能１５０、クライアントインターフェースモジュール１２２、メタデータ監視拡張機能１１４、および監査インターフェース１１８を含むプライバシーメタデータサービスインターフェース８０２が、データベース管理システム１０４への全アクセス途上に配置される。それゆえ、プライバシーメタデータサービスインターフェース１２０２は、データベース管理システム１０４、データビュースイート１０８内のデータビュー、およびマクロスイート１１１内のマクロへのすべてのアクセスのログ記録を取り、アクセスを制御することができる。

【００９０】図１２はプライバシーメタデータサービス機能インターフェースが介在するデータビューの実施例を示す図である。データベース管理システム１０４の顧客ベース表内のデータの可視性およびデータへのアクセスはデータビューおよびマクロ１１１により与えられる。データの中に入って行われる閲覧は図１２に示す共心的四角形で表してある。消費者アクセスマクロもしくは消費者ビューは、その消費者もしくはデータ主体に関するデータを収容する消費者データベース表の単一行へのアクセスをユーザー／消費者に与える。データベースのインフラストラクチャーの定義と管理維持はシステムアシスタント１２０２がサポートし、それらの表、データビュー、マクロ、ユーザープロファイル、ログ、監査レポートはプライバシーアシスタント１２０４がサポートする。前述の場合と同様、ルーチンアプリケーション１１０Ａは標準ビュー２６０を介して、また解析アプリケーション１１０Ｃは匿名ビューを介して、顧客ベース表にアクセスする。ただしこの場合、顧客の身元を同定できるデータは隠される。処置アプリケーション（マーケティング アプリケーション）１１０Ｄは顧客データの全行が省かれる適用除外選択ビューを介してアクセスし、サードパーティ公開アプリケーション（third party disclosure applications）１１２に提供されるデータビューは、適用選択をした顧客のみを提示するが身元同定データへのアクセスは許可しない。適用除外選択ビュー／匿名データビューは別個に用意したデータビューで提供することができ、あるいは適用除外選択および匿名化の両方を適用するデータビューで与えることができる。

【図面の簡単な説明】

【図１】データウェアハウス化システム実施例のシステムブロック図である。

【図２】プライバシー拡張顧客表およびデータベースビュー内に格納された顧客表の構造例を示すブロック図で

25

ある。

【図３】データウェアハウス化システムの別の実施例のシステムブロック図である。

【図４】本発明の特徴であるプライバシー監査オペレーションの概略を表すブロック図である。

【図５】本発明の一実施例を実行するために使用されるオペレーション例を示す流れ図である。

【図６】顧客を同定する顧客固有プロキシをデータウェアハウスに格納するのに使用するオペレーションの実施例を示す流れ図である。

【図７】顧客を同定する顧客固有プロキシをデータウェアハウスに格納するのに使用するオペレーションのもう一つの実施例を示す流れ図である。

【図８】愛顧者カードで取引を行うのに使用するオペレーション例を示す流れ図である。

【図９】愛顧者カードで顧客のプライバシープレファレンスを管理するために使用するオペレーション例を示す流れ図である。

【図１０】別途用意された信託データベースを備えたプライバシーデータウェアハウスの別の実施例を示す図である。

【図１１】全データアクセスを管理しログ記録を取るために挿入されたプライバシーメタデータサービス機能インターフェースを備えたプライバシーデータウェアハウスの別の実施例を示す図である。

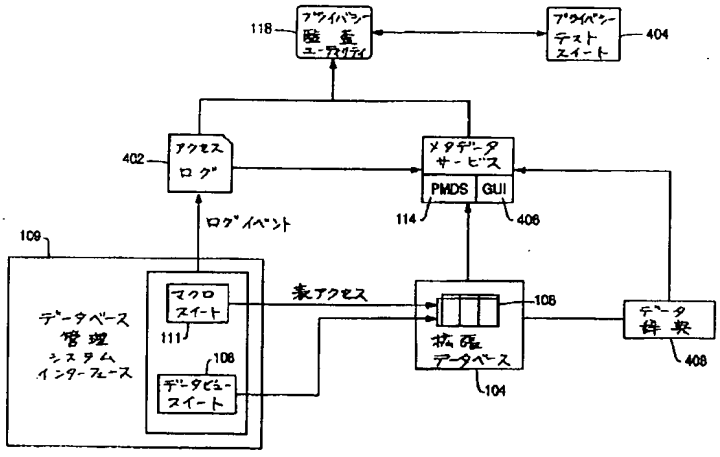
【図１２】プライバシーメタデータサービス機能インターフェースを挿入されたデータビューの設置例を示す図である。

26

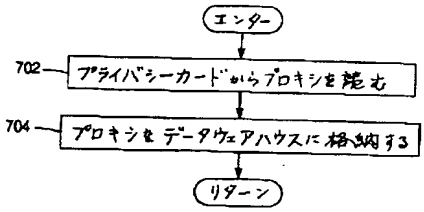
【符号の説明】

１００	データウェアハウス化システム
１０２	保安データウェアハウス（secure data warehouse）
１０４	データベース管理システム（database management system）
１０６	拡張データベース
１２８	ブラウザプラグイン
２０２	顧客表
２０４	同定情報部分
２０６	個人情報部分
２０８	機密情報部分
２１０	グローバルデータ制御列
２１２	データ制御列
１００２	格納表
１００４	信託データベース
１１０２	プライバシーメタデータサービスインターフェース
１２０４	プライバシーアシスタント

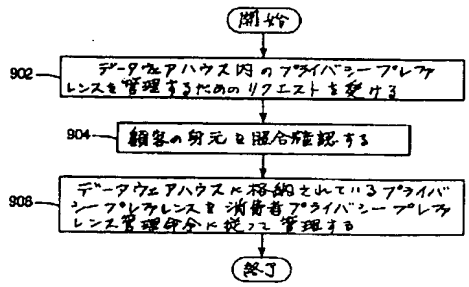
【図４】



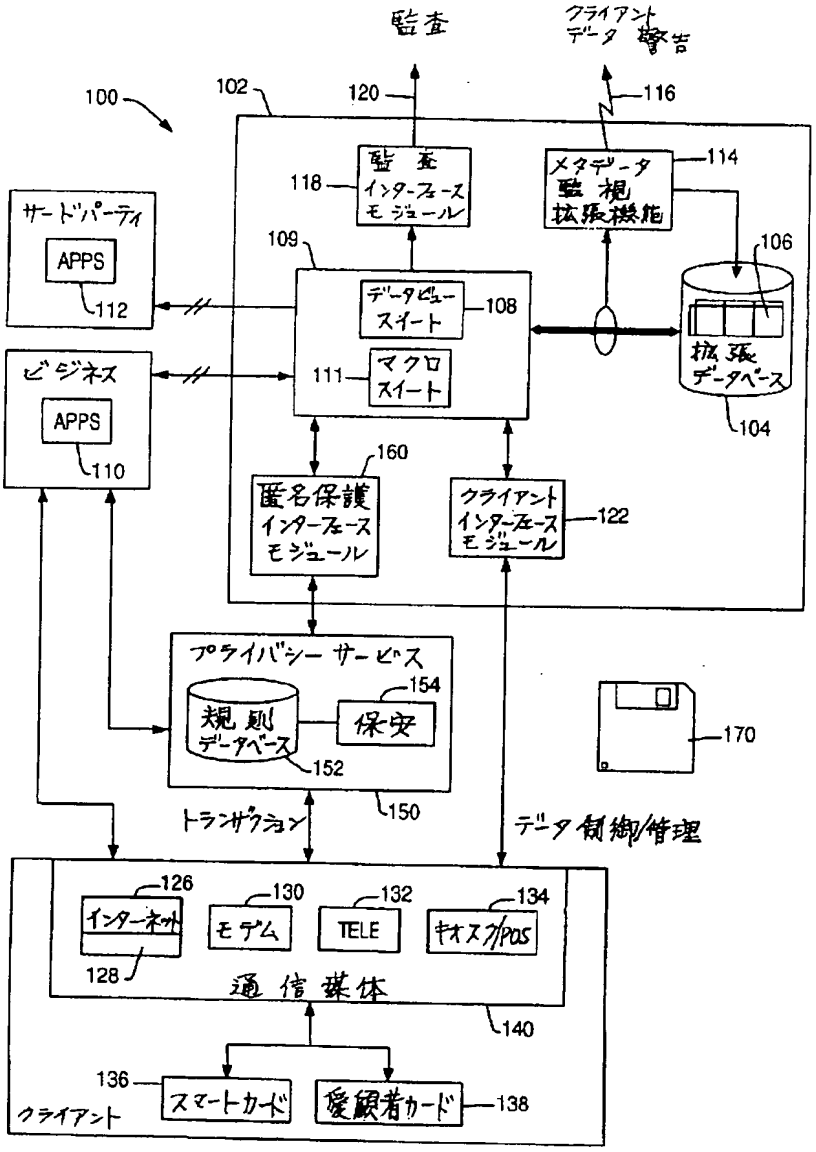
【図７】



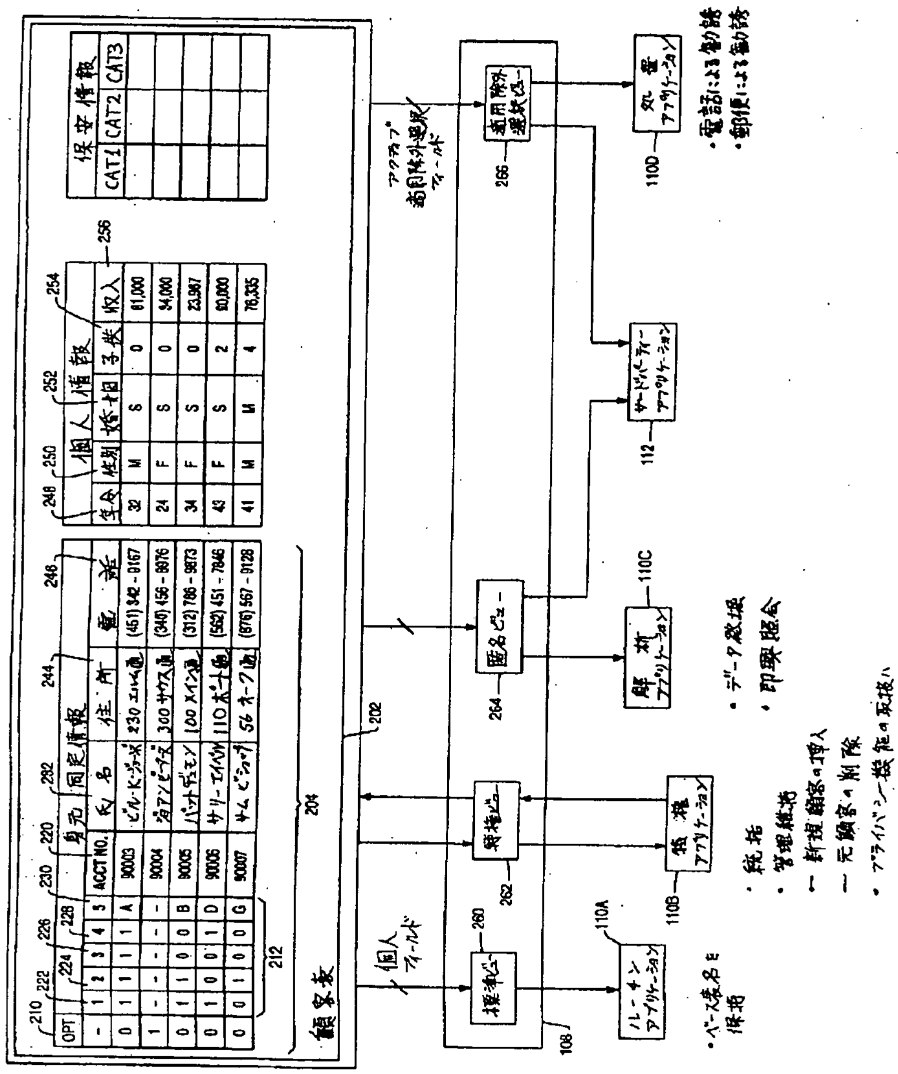
【図９】



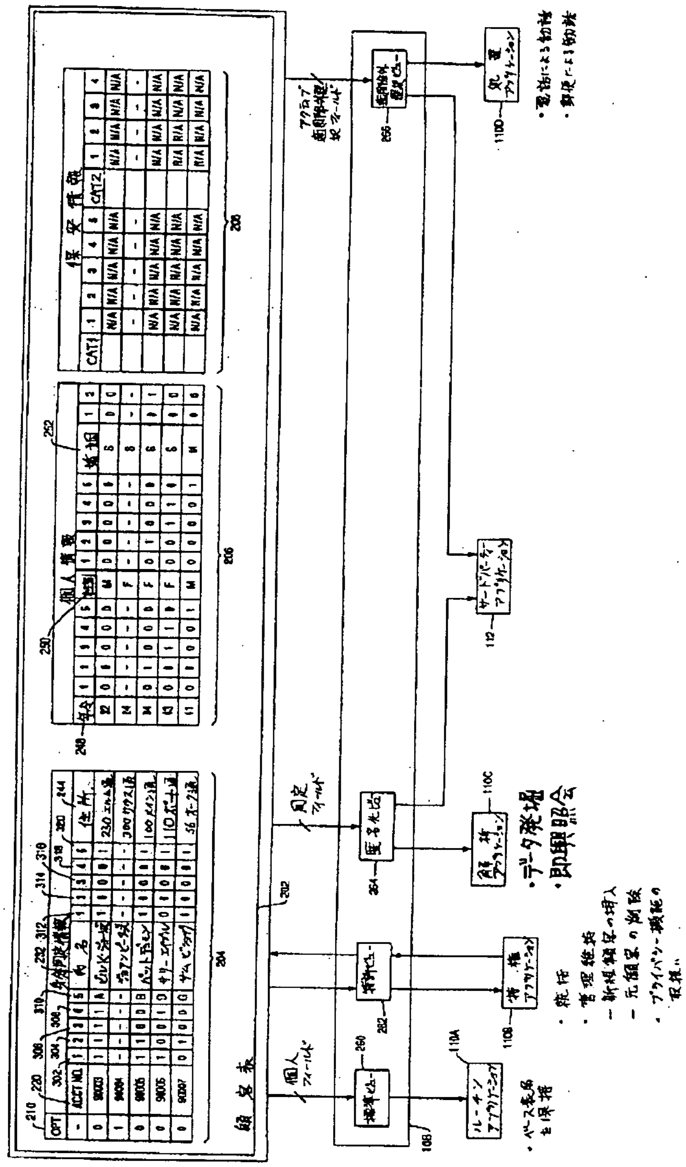
【図１】


監査
クライアント データ 警告
100
102
120
116
監査 インターフェース モジュール
118
メタデータ 監視 拡張機能
114
サードパーティ
APPS
112
109
データビュー スイート
108
106
拡張 データベース
104
ビジネス
APPS
110
111
マクロ スイート
160
匿名保護 インターフェース モジュール
クライアント インターフェース モジュール
122
プライバシー サービス
154
規則 データベース
保安
152
150
170
トランザクション
データ制御/管理
126
130
132
134
インターネット
モデム
TELE
キオスク/POS
128
通信媒体
140
136
スマートカード
優顧着カード
138
クライアント

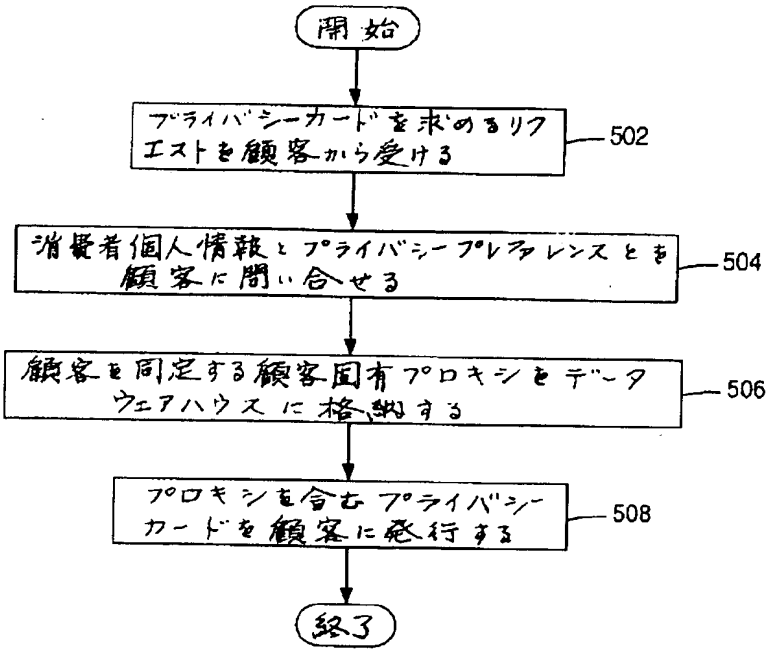
【図２】


顧客表
保安情報
CAT1
CAT2
CAT3
個人情報
ACCT NO.
OPT
210
222
224
226
228
230
220
282
244
246
248
250
252
254
256
212
204
202
108
260
262
264
266
110A
110B
110C
110D
112

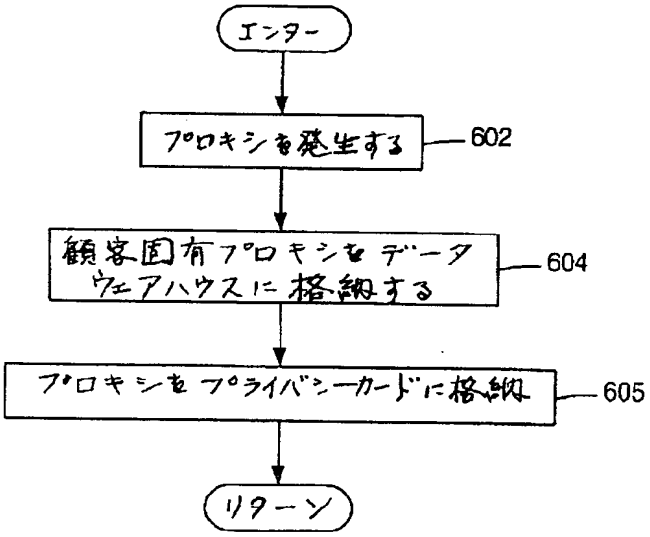
【図３】



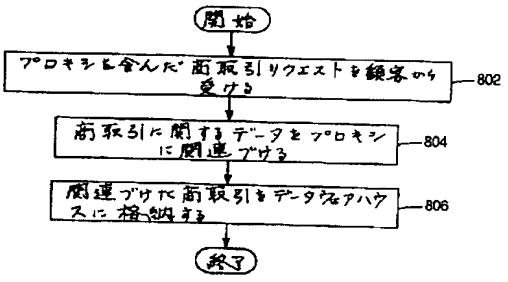
【図５】


開始
プライバシーカードを求めるリクエストを顧客から受ける
502
消費者個人情報とプライバシープレファレンスとを顧客に問い合せる
504
顧客を同定する顧客固有プロキシをデータウェアハウスに格納する
506
プロキシを含むプライバシーカードを顧客に発行する
508
終了

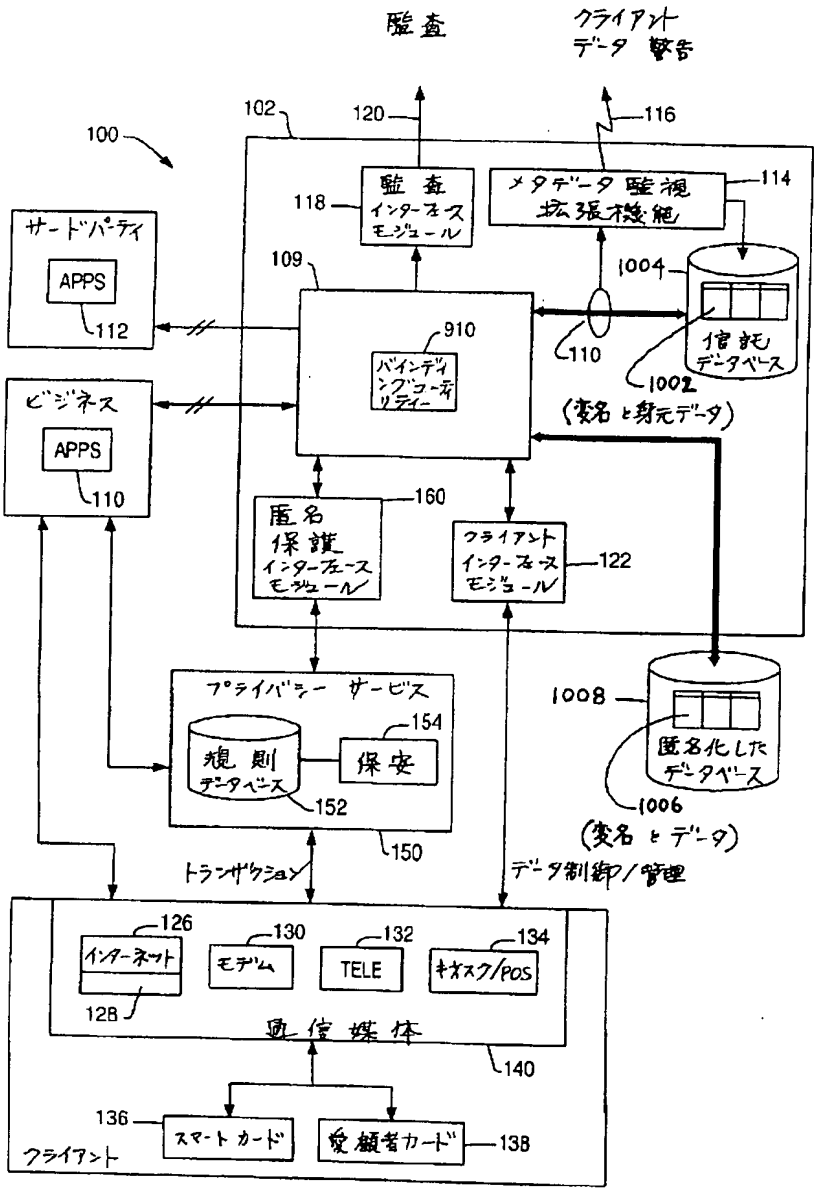
【図６】


エンター
プロキシを発生する
602
顧客固有プロキシをデータウェアハウスに格納する
604
プロキシをプライバシーカードに格納
605
リターン

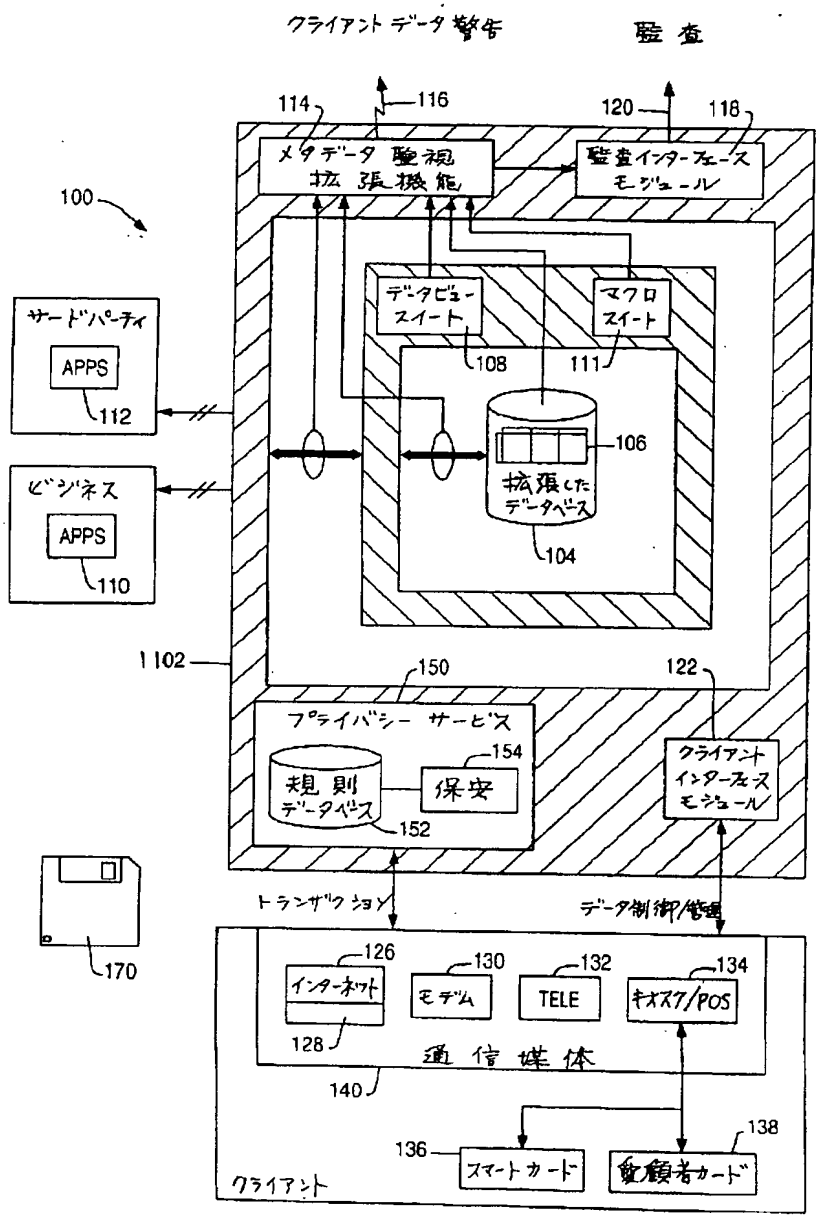
【図８】


開始
プロキシを含んだ商取引リクエストを顧客から受ける
802
商取引に関するデータをプロキシに関連づける
804
関連づけた商取引をデータウェアハウスに格納する
806
終了

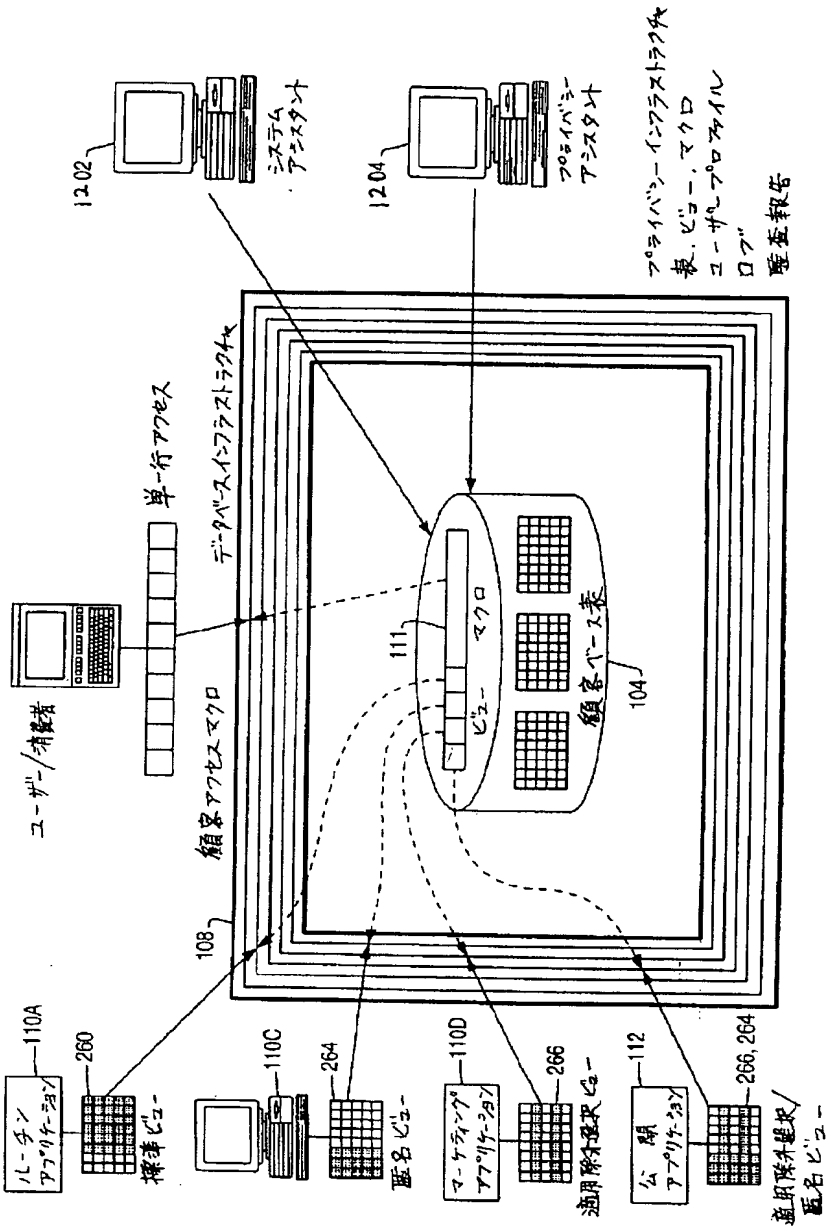
【図１０】


監査
クライアント
データ 報告
100
102
120
116
118
監査 インターフェース モジュール
メタデータ 監視 拡張機能
114
サードパーティ
APPS
112
109
1004
910
バインディング コーディネイター
110
信託 データベース
1002
(変名と身元データ)
ビジネス
APPS
110
匿名 保護 インターフェース モジュール
160
クライアント インターフェース モジュール
122
プライバシー サービス
154
規則 データベース
保安
152
150
1008
匿名化した データベース
1006
(変名とデータ)
トランザクション
データ制御/管理
126
130
132
134
インターネット
モデム
TELE
キオスク/POS
128
通信媒体
140
136
スマートカード
受領者カード
138
クライアント

【図１１】


クライアント データ 警告
監査
114
116
120
118
メタデータ 監視 拡張機能
監査インターフェース モジュール
100
データビュー スイート
マクロ スイート
108
111
106
拡張した データベース
104
サードパーティ
APPS
112
ビジネス
APPS
110
1102
150
122
プライバシー サービス
154
規則 データベース
保安
152
クライアント インターフェース モジュール
トランザクション
データ制御/管理
170
126
130
132
134
インターネット
モデム
TELE
キオスク/POS
128
通信媒体
140
136
138
スマートカード
顧客カード
クライアント

【図１２】



フロントページの続き

(72)発明者　ケネス　ダブリュー　オフラハティー
アメリカ合衆国　92130　カリフォルニア州　サン　ディエゴ　トリー　ビュー　コート　3765

(72)発明者　レイド　エム　ワッツ
アメリカ合衆国　29072　サウスキャロライナ州　レキシントン　スプリング　クリーク　コート　201

(72)発明者　デビッド　エー　ラムゼイ
アメリカ合衆国　29072　サウスキャロライナ州　レキシントン　ベレ　チェイス　ドライブ　124

【外国語明細書】

1 Title of Invention

PRIVACY-ENABLED LOYALTY CARD SYSTEM AND METHOD

2 Claims

1. A method of controlling the collection and dissemination of data stored in a data warehouse, characterized by the steps of:

accepting a request for a privacy card from a consumer;

querying the consumer for consumer personal information and privacy preferences;

storing a customer unique proxy identifying the customer in the data warehouse; and

issuing a privacy card comprising the proxy to the customer.

2. The method of claim 1, wherein the step of storing a customer unique proxy in the data warehouse comprises the steps of:

generating the proxy;

storing the customer unique proxy in the data warehouse; and

storing the proxy in the privacy card.

3. The method of claim 2, wherein the privacy card is a smart card.

4. The method of claim 1, wherein the step of storing a customer unique proxy in the data warehouse comprises the steps of:

reading the proxy from the privacy card; and

storing the proxy in the data warehouse.

5. The method of claim 1, further comprising the steps of:

receiving a request for a commercial transaction from the consumer, the request comprising the proxy;

associating data about the commercial transaction with the proxy; and

storing the associated commercial transaction data in the data warehouse.

6. The method of claim 1, further comprising the steps of:

accepting a request from the consumer to manage the privacy preferences in the data warehouse; and

verifying the identity of the consumer; and

managing the privacy preferences stored in the data warehouse in accordance with a consumer privacy preference management command.

7. The method of claim 1, wherein the proxy is stored in the data warehouse secure from the consumer personal information.

8. The method of claim 1, wherein a customer unique identification code for is generated and stored for each of a plurality of retailers.

9. An apparatus for controlling the collection and dissemination of data stored in a data warehouse, characterized by :

means for accepting a request for a privacy card from a consumer;

means for querying the consumer for consumer personal information and privacy preferences;

means for storing a customer unique proxy identifying the customer in the data warehouse; and

means for issuing a privacy card comprising the proxy to the customer.

10. The apparatus of claim 9, wherein the means for storing a customer unique proxy in the data warehouse comprises:

means for generating the proxy;

means for storing the customer unique proxy in the data warehouse; and

means for storing the proxy in the privacy card.

11. The apparatus of claim 10, wherein the privacy card is a smart card.

12. The apparatus of claim 9, wherein the means for storing a customer unique proxy in the data warehouse comprises:

means for reading the proxy from the privacy card; and

means for storing the proxy in the data warehouse.

13. The apparatus of claim 9, further comprising:

means for receiving a request for a commercial transaction from the consumer, the request comprising the proxy;

means for associating data about the commercial transaction with the proxy; and

means for storing the associated commercial transaction data in the data warehouse.

14. The apparatus of claim 9, further comprising:

means for accepting a request from the consumer to manage the privacy preferences in the data warehouse; and

means for verifying the identity of the consumer; and

means for managing the privacy preferences stored in the data warehouse in accordance with a consumer privacy preference management command.

15. The apparatus of claim 9, wherein the proxy is stored in the data warehouse secure from the consumer personal information.

16. The apparatus of claim 9, wherein a customer unique identification code for is generated and stored for each of a plurality of retailers.

17. A program storage device, readable by a computer, embodying one or more instructions executable by the computer to perform method steps for controlling the collection and dissemination of data stored in a data warehouse, the method steps characterized by the steps of:

accepting a request for a privacy card from a consumer;

querying the consumer for consumer personal information and privacy preferences;

storing a customer unique proxy identifying the customer in the data warehouse; and

issuing a privacy card comprising the proxy to the customer.

18. The program storage device of claim 17, wherein the method step of storing a customer unique proxy in the data warehouse comprises the method steps of:

generating the proxy;

storing the customer unique proxy in the data warehouse; and

storing the proxy in the privacy card.

19. The program storage of claim 18, wherein the privacy card is a smart card.

20. The program storage device of claim 17, wherein the method step of storing a customer unique proxy in the data warehouse comprises the method steps of:

reading the proxy from the privacy card; and

storing the proxy in the data warehouse.

21. The program storage device of claim 17, wherein the method steps further comprise the method steps of:

receiving a request for a commercial transaction from the consumer, the request comprising the proxy;

associating data about the commercial transaction with the proxy; and

storing the associated commercial transaction data in the data warehouse.

22. The program storage device of claim 17, wherein the method steps further comprising the method steps of:

accepting a request from the consumer to manage the privacy preferences in the data warehouse; and

verifying the identity of the consumer; and

managing the privacy preferences stored in the data warehouse in accordance with a consumer privacy preference management command.

23. The program storage device of claim 17, wherein the proxy is stored in the data warehouse secure from the consumer personal information.

24. The program storage device of claim 17, wherein a customer unique identification code for is generated and stored for each of a plurality of retailers.

6

3 Detailed Description of Invention

The present invention relates to systems and methods of data warehousing and analysis, and in particular to a system and method for enforcing privacy constraints on a database management system.

Database management systems are used to collect, store, disseminate, and analyze data. These large-scale integrated database management systems provide an efficient, consistent, and secure data warehousing capability for storing, retrieving, and analyzing vast amounts of data. This ability to collect, analyze, and manage massive amounts of information has become a virtual necessity in business today.

The information stored by these data warehouses can come from a variety of sources. One important data warehousing application involves the collection and analysis of information collected in the course of commercial transactions between businesses and consumers. For example, when an individual uses a credit card to purchase an item at a retail store, the identity of the customer, the item purchased, the purchase amount and other related information are collected. Traditionally, this information is used by the retailer to determine if the transaction should be completed, and to control product inventory. Such data can also be used to determine temporal and geographical purchasing trends.

Similar uses of personal data occur in other industries. For example, in banking, the buying patterns of consumers can be divined by analyzing their credit card transaction profile or their checking/savings account activity, and consumers with certain profiles can be identified as potential customers for new services, such as mortgages or individual retirement accounts. Further, in the telecommunications industry, consumer telephone calling patterns can be analyzed from call-detail records, and individuals with certain profiles can be identified for selling additional services, such as a second phone line or call waiting.

Additionally, data warehouse owners typically purchase data from third parties, to enrich transactional data. This enrichment process adds demographic data such as household membership, income, employer, and other personal data.

The data collected during such transactions is also useful in other applications. For example, information regarding a particular transaction can be correlated to personal information about the consumer (age, occupation, residential area, income, etc.) to generate statistical information. In some cases, this personal information can be broadly classified into two groups: information that reveals the identity of the consumer, and information that does not. Information that does not reveal the identity of the consumer is useful because it can be used to generate information about the purchasing proclivities of consumers with similar personal characteristics. Personal information that reveals the identity of the consumer can be used for a more focused and personalized marketing approach in which the purchasing habits of each individual consumer are analyzed to identify candidates for additional or tailored marketing.

Another example of an increase in the collection of personal data is evidenced by the recent proliferation of "membership" or "loyalty" cards. These cards provide the consumer with reduced prices for certain products, but each time the consumer uses the card with the purchase, information about the consumer's buying habits is collected. The same information can be obtained in an on-line environment, or purchases with smart cards, telephone cards, and debit or credit cards.

Unfortunately, while the collection and analysis of such data can be of great public benefit, it can also be the subject of considerable abuse. In the case of loyalty programs, the potential for such abuse can prevent many otherwise cooperative consumers from signing up for membership awards or other programs. It can also discourage the use of emerging technology, such as cash cards, and foster continuation of more conservative payment methods such as cash and checks. In fact, public concern over privacy is believed to be a factor holding back the anticipated explosive growth in web commerce.

For all of these reasons, as well as regulatory constrains, when personal information is stored in data warehouses, it is incumbent on those that control this data to protect the data from such abuse. As more and more data is collected in this, the computer age, the rights of individuals regarding the use of data pertaining to them have become of greater importance.

It is an object of the present invention to provide a system and method which provides all the advantages of a complete data warehousing system, while addressing the privacy concerns of the consumer.

From a first aspect, the present invention resides in a method of controlling the collection and dissemination of data stored in a data warehouse, characterized by the steps of:

accepting a request for a privacy card from a consumer;

querying the consumer for consumer personal information and privacy preferences;

storing a customer unique proxy identifying the customer in the data warehouse; and

issuing a privacy card comprising the proxy to the customer.

From a second aspect, the present invention resides in an apparatus for controlling the collection and dissemination of data stored in a data warehouse, characterized by :

means for accepting a request for a privacy card from a consumer;

means for querying the consumer for consumer personal information and privacy preferences;

means for storing a customer unique proxy identifying the customer in the data warehouse; and

means for issuing a privacy card comprising the proxy to the customer.

From a third aspect, the present invention resides in a program storage device, readable by a computer, embodying one or more instructions executable by the computer to perform method steps for controlling the collection and dissemination of data stored in a data warehouse, the method steps characterized by the steps of:

accepting a request for a privacy card from a consumer;

querying the consumer for consumer personal information and privacy preferences;

storing a customer unique proxy identifying the customer in the data warehouse; and

issuing a privacy card comprising the proxy to the customer.

One embodiment of the present invention also utilizes a privacy metadata system that administers and records all data, users, and usage of data that is registered as containing privacy elements.. This metadata service provides for locating, consolidating, managing, and navigating warehouse metadata. It also allows for setting aside an area from which all system aspects of privacy are registered, administered, and logged in an auditable format.

Embodiments of the present invention will now be described by way of reference only to the accompanying drawings.

Overview

FIG. 1 is a system block diagram presenting an overview of a data warehousing system 100. The system comprises secure data warehouse 102 having a database management system 104 storing one or more extended databases 106 therein.

One important capability of a database management system is the ability to define a virtual table and save that definition in the database as metadata with a user-defined name. The object formed by this operation is known as a View or a database view (the particular database views used in the present invention are hereinafter referred to as "dataviews"). As a virtual table, a dataview is not physically materialized anywhere in the database until it is needed. All accesses to data, (with the possible exception of data access for administrative purposes) is accomplished through dataviews. To implement a variety of privacy rules, a suite of a plurality of dataviews is provided. Metadata about the privacy dataviews (including the dataview name, names and data types of the dataview columns, and the method by which the rows are to be derived) is stored persistently in the databases metadata, but the actual data presented by the view is not physically stored anywhere in association with the derived table. Instead, the data itself is stored in a persistent base table, and the view's rows are derived from that base table. Although the dataview is a virtual table, operations can be performed against dataviews just as they can be performed against the base tables.

The secure data warehouse 102 further comprises a suite of privacy metadata dataviews 108 through which all data in the extended database 106 are presented. Data within the extended database 106 can be viewed, processed, or altered only through the dataviews in this suite. The schema and logical model of the extended database and dataviews is set forth more fully herein with respect to FIG. 2.

Virtually all access to the data stored in the extended database 106 is provided solely through the dataview suite 108. Thus, business applications 110 and third party applications 112 have access only to such data as permitted by the database view provided. In one embodiment, provision is made to permit override of the customer's privacy

preferences. However, in such circumstances, data describing the nature of the override is written to the database for retrieval by the audit module 118, so that the override cannot occur surreptitiously. Further, overrides may be monitored by the privacy metadata monitoring extensions 114 to provide an alert to the consumer when such overrides occur.

The limiting access to the data stored in the extended database 106 to access provided by the privacy dataview suite 108 for purposes of (1) implementing privacy rules provides the capability to make the personal data anonymous (through the anonymizing view described herein), (2) to restrict access to opted-out columns, which can apply to all personal data, separate categories of personal data, or individual data columns, and (3) to exclude entire rows (customer records) for opt-out purposes based on customer opt-outs (excluding a row if any of the applicable opt-out flags has been set for the customer in question, thus preventing any direct marketing or disclosure to third parties).

Using a client interface module 122 that communicates with the dataviews 108, a client 124 can access, control, and manage the data collected from the client 124. This data control and management can be accomplished using a wide variety of communication media 140, including the Internet 126 (via a suitable browser plug-in 128, a modem 130, voice telephone communications 132, or a kiosk 134 or other device at the point of sale. To facilitate such communications, the kiosk or other device at the point of sale, can issue a smartcard 136 or a loyalty card 138. The kiosk/pos device 134 can accept consumer input regarding privacy preferences, and issue a smartcard 136 or loyalty card 138 storing information regarding these preferences. Similarly, the using the kiosk/pos device 134 and the smartcard 136 or loyalty card 138, the consumer may update or change preferences as desired. In cases where the loyalty card 138 is a simple read only device (such as a bar-coded attachment to a key ring), the kiosk/pos device 134 can issue replacement cards with the updated information as necessary. Transactions using the loyalty card 138 or smartcard 136 are selectably encrypted and anonymous. Either card may interact directly with the server or through a plug-in to implement the security rules selected.

Through this interface, the consumer can specify data sharing and retention preferences. These preferences include data retention preferences, and data sharing preferences. These allow the consumer to specify when and under what circumstances personal information may be retained or shared with or sold to others. For example, the

consumer may permit such data retention as a part of a loyalty card program, or if the use of the data is limited to particular uses. Further, the consumer may specify under what circumstances the data may be sold outright, used for statistical analysis purposes, or used for third party elective marketing programs.

The data warehousing system 100 also permits anonymous communication between the client and the secure data warehouse 102 via a privacy service 150. When the user desires an anonymous transaction, the transaction is routed to the privacy service 150. The privacy service 150 accesses a privacy rule database 152 and other security information 154 and uses the privacy rule and security information to remove all information from which the identity of the consumer can be determined. The cleansed transaction information is then forwarded to the anonymity protection interface module 160 in the secure data warehouse. Communications with the secure data warehouse 102 use a proxy user identification, which is created by the privacy service 150 from the customer's username or other identifying information. If the customer does not require an anonymous transaction, the transaction is provided directly to the retailer who may store the transaction information in the extended database.

Since it alone provides access to data within the extended database, the dataview suite 108 also provides a convenient and comprehensive means for auditing the security of the secure data warehouse 102.

The secure data warehouse 102 also comprises metadata monitoring extension 114. This extension 114 allows the customer to generate a rule to monitor the use of personal data, and to transmit an alert 116 or callback if a metadata definition change occurs. The consumer can control the metadata monitoring extension 114 to trigger an alert when the customer's personal information is read from the extended database 106, is written to the extended database 106, if the opt-out delimiters stored in the extended database are changed, or when a table,or a dataview is accessed. Alternatively, triggered alerts can be logged for later access by the consumer.

The metadata monitoring extension 114 also records data source information, so customers can determine the source of the data stored in the secure data warehouse 102. The data source may be the customer, or may be a third party intermediary source. This feature is particularly useful when the consumer would like to not only correct erroneous

information, but to determine the source of the erroneous information so the error will not be replicated in the same database or elsewhere.

Source data may also be stored in the data table for each column or set of columns so that the source of the data can be ascertained directly from table data. In this embodiment, the source identification is generalized so that each customer can have a different source of information without the need to replicate information source information in the metadata for all customers.

Similarly, the metadata monitoring extension 114 also records data target information, so that customers can determine who has been a recipient of their personal information. This feature is also useful for correcting replicated errors, as well as for monitoring disclosure activity relative to a consumer's personal information.

The metadata monitoring extension 114 can also be used to support auditing functions by tracking reads or writes from the extended database 106 as well as the changes to the dataview suite 108.

The present invention can be implemented in a computer comprising a processor and a memory, such as a random access memory (RAM). Such computer is typically operatively coupled to a display, which presents images such as windows to the user on a graphical user interface. The computer may be coupled to other devices, such as a keyboard, a mouse device, a printer, etc. Of course, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the computer.

Generally, the computer operates under control of an operating system stored in the memory, and interfaces with the user to accept inputs and commands and to present results through a graphical user interface (GUI) module. Although the GUI module is typically a separate module, the instructions performing the GUI functions can be resident or distributed in the operating system, an application program, or implemented with special purpose memory and processors. The computer may also implement a compiler that allows an application program written in a programming language such as COBOL, C++, FORTRAN, or other language to be translated into processor-readable code. After completion, the application accesses and manipulates data stored in the memory of the computer using the relationships and logic that was generated using the compiler.

In one embodiment, instructions implementing the operating system, the computer program, and the compiler are tangibly embodied in a computer-readable medium, e.g., data storage device 170, which could include one or more fixed or removable data storage devices, such as a zip drive, floppy disc drive, hard drive, CD-ROM drive, tape drive, etc. Further, the operating system and the computer program are comprised of instructions which, when read and executed by the computer, causes the computer to perform the steps necessary to implement and/or use the present invention. Computer program and/or operating instructions may also be tangibly embodied in memory and/or data communications devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "program storage device," "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program accessible from any computer readable device or media.

Those skilled in the art will recognize many modifications may be made to this configuration without departing from the scope of the present invention. For example, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the present invention.

Logical Model

FIG. 2 is a diagram showing an exemplary logical model of the secure data warehouse 102 and the dataview suite 108 in greater detail. The extended database 106 comprises a customer table 202, which is segmented into three portions: an identity information portion 204, a personal information portion 206, and a sensitive information portion 208. The identity information portion 206 comprises data columns 220, 232, 244, and 246, which store information that reveals the identity of the consumer. These columns include a consumer account number column 220, name column 232, an address column 244, and a telephone number column 246. The identity portion 204 of the customer table 202 also comprises one or more data control columns 212, which specify data reflecting the privacy preferences, or "opt-outs" for the accompanying data. In the illustrated embodiment, columns 222-230 stores one or more characters ("A" or "D") or flags (represented by "1s" and "0s") which specify privacy preferences for the consumer's data

records. In the disclosed embodiment, these privacy preferences include "opt-outs" for (1) direct marketing, (2) disclosure of personal data along with information identifying the consumer, (3) anonymous disclosure of personal data, (4) disclosure of personal data for purposes of making automated decisions, and (5) disclosure or use of sensitive data. The customer table 202 also comprises a global data control column 210. This column can be used to indicate that the consumer wants maximum privacy.

In the exemplary embodiment illustrated, a consumer named Bill K. Jones has permitted some data collection, analysis, or dissemination by selecting a "0" in the global data control column 210. He has further indicated that his consumer information can be used in direct marketing and can be disclosed to third parties, both with his identity, and anonymously. He has allowed the data to be used to perform automated processing, and will permit the dissemination of sensitive data.

In one embodiment, a TERADATA database management system is utilized to implement the foregoing logical model. This implementation has several advantages.

First, TERADATA's ability to store and handle large amounts of data eases the construction of the many different views and allows the secure data warehousing system 100 to utilize a logical data model in or close to the third normal form.

Second, unlike systems which execute SQL queries as a series of selections to narrow the data down to the dataview subset, the TERADATA database management system rewrites dataview-based queries to generate the SQL that selects the necessary columns directly from the appropriate base tables. While other views materialize entire tables before narrowing down the data to the view subset, TERADATA generates SQL that selectively pulls appropriate columns and rows into the result table. This method is a particularly advantageous in implementing the foregoing logical model.

Third, the foregoing logical model generally results in dataviews, which include complex queries and wide SQL expressions. The TERADATA database management system is particularly effective at optimizing such queries and SQL expressions.

Using the foregoing teaching, alternative logical models having alternatively defined data control column structures can be implemented to meet the particular privacy granularity and control needs of each database application.

Dataviews

A number of dataviews are provided in the dataview suite 108. These dataviews include a standard view 260, a privileged view 262, an anonymizing view 264, and an opt-out view 266. These views limit visibility into the data in the customer table 202 in accordance with the values placed in the data control columns 212.

The standard view 260 will not present personal data unless either the flag in column 224 (indicating that the personal information and identifying information can be disseminated) or 226 (indicating that personal information can only be disseminated anonymously) is activated. Hence, the standard view 260 selectively masks personal data from view unless the consumer has had the appropriate flags set to the proper value.

Scaleable data warehouse (SDW) customer database administrators (DBAs) set up views into customer tables (any tables containing personal information about their customers), such that, for routine users, all columns of personal information are hidden. This allows all routine decision support (DSS) applications and tools with query access to the warehoused data to be precluded from viewing personal information and consequently, all end-users of these applications and tools are also precluded from viewing personal information as well.

To minimize disruption to existing SDW customers, dataviews are established using the same names that are used for base tables in any existing applications that access private data, and corresponding base table names can be renamed to some other value. Thus, whenever an existing application attempts to access private data (now via a dataview), the private data can be screened out by the dataview, depending on user privileges. Using this approach, there is no need to modify existing applications. Instead, the logical data model and database schema would be modified, and additional naming conventions would be introduced.

The privileged view 262 permits viewing, analysis, and alteration of all information. The privileged view 262 will be supplied only to privileged (Class "A" applications 110B, such as those required for administration and/or maintenance of the database (e.g. for inserting new customers, deleting ex-customers, handling address changes), and to those applications which handle privacy related functions (such as informing customers about personal information collected about them, changing/updating personal information, and

applying "Opt-in/Opt-out" controls). For example, the client interface module 212, which is used to view, specify, and change consumer privacy preferences, is a privileged application. Appropriate security measures are undertaken to assure that the privileged applications are suitably identified as such, and to prevent privileged view 262 access by any entity that is not so authorized.

Certain SDW applications ("Class B") may perform analysis on personal data, in order to gain insight into customer behavior, e.g. to identify trends or patterns. Such applications may be driven by end-users (knowledge workers or "power analysts") performing "ad hoc" queries, typically using either custom-built software or standard query or OLAP Tools, where the end-user spots the patterns. They may also involve the use of data mining tools, where statistical or machine learning algorithms, in conjunction with the analyst, discover patterns and from them build predictive models.

To derive the greatest value, analytic applications must have access to all available forms of personal information. In order to enable such access, while at the same time respecting personal privacy requirements, special "anonymizing" dataviews are used. These dataviews are designed to provide access to personal data fields, but to screen out all fields containing information that can identify the owner of the data (e.g. name, address, phone number, social security number, account numbers).

The anonymizing view 264 permits the viewing and analysis of personal information, but screens the information stored in the identity information portion 204 from view or analysis unless the flag in the column 224 (permitting disclosure of personal data along with information identifying the consumer) is selected. This data can be provided to analytic applications 110C, which permit data mining and ad-hoc queries. If the consumer permits, this information may also be provided to third party applications 112.

A further class of privileged applications ("Class C") includes applications that use personal information to take some form of action, such as marketing applications (e.g. to create mail or phone solicitations). These marketing applications are subject to the "Opt-in/Opt-out" controls set for each customer, and access customer information through a special dataview that removes or masks all records associated with an activated "Opt-out" indicator. Thus, for example, any customer who has opted out from receiving marketing solicitations would be omitted from any contact list created by the marketing application.

The "Opt out" indicator is a new column added to customer tables, or joined to existing customer tables via dataviews (which is an additional change to the logical data model). In one embodiment, the value of this column for each customer row is initially be set to "Opt Out" (or "Opt in" if permitted by law), and can be modified via the client interface module 122, which handles customer requests regarding privacy controls.

Multiple "Opt Out" indicators may be set up for each customer record. At a minimum, five opt-outs are implemented: for "direct marketing", "third-party disclosure of identifiable data", "third-party disclosure of anonymous data", automated decisions", and "use of sensitive data". However, a scheme of more fine-grained opt-outs could be designed, based on more detailed customer preferences. For example, "direct marketing" could be broken out into separate opt-outs for contact by telephone, direct mail, and electronic mail, and a catchall for "other" action. This would yield eight separate opt-outs.

Opt-out view 266 permits the use of information for purposes of making automated decisions with action applications 110D, such as those which implement phone or mail solicitation. Views into this information are controlled by the flag in column 228. Alternatively, the value stored in column 228 may comprise a character with sufficient range to permit the single character to not only define that solicitation is permitted, but to indicate what kind and scope of permitted solicitation.

Applications or queries that disclose personal data to third parties (e.g. for marketing or analytic purposes) are subject to both the Class C ("Opt Out") and Class B ("anonymizing") Views. If the customer has opted out of third-party use of their data, then the "Opt Out" dataview applies, and their row (record) is excluded from the output. Other customers may have opted in to third-party disclosure of their data provided it is anonymous; in these cases, the customer data is made anonymous via the "anonymizing" dataview before being output. In all other cases, the customer has opted in to disclosure of their personal data in identifiable form; here the personal data is output along with identifying data columns.

A more fine-grained approach to opting in or out may be implemented. Specific opt-ins or opt-outs could be agreed with each customer for a variety of permissions and protections. For example, disclosure to third parties could be based on specific data fields, relating both to personal characteristics and to personal identifications: a customer might

agree to their address and interest profile being provided, but not their financial information and their phone number.

Opt-in/opt-out could also be further extended to gain a more detailed profile of each customer and their interests. For example, each class of opt-out (e.g. the eight opt-outs identified in section 4) could be applied separately to each category of personal data (e.g. demographic data; preference data), or down to each specific data item of personal data (e.g. age, gender; hiking interest, shoe brand preference). In this manner, customers could opt out of certain actions relating to certain interest areas, but could opt in to others (e.g. to receive direct mail marketing for running shoes).

FIG. 3 is a diagram showing an alternative logical model of the secure data warehouse 102 with more fine-grained opt-ins and opt-outs. In this embodiment, each class of privacy preference is applied separately to each category of data (e.g. demographics), or down to each specific data item of personal data (e.g. age, gender, hiking interest, or shoe brand preference). For example, consumer Bill K. Jones may elect to allow his name to be accessible for some purposes, but not others. These limitations can be selected by entering the proper combination of flags for the entries in columns 302-310. Similarly, columns 312-320 can be used to specify the privacy preferences with regard to the storage and/or use of Mr. Jones' name. The preferences defined in columns 312-320 may be different or the same as those described in columns 302-310. The present invention also permits the expansion of the foregoing security preference paradigm to a system of multiple fine-grain preferences, based upon more detailed customer preferences. For example, direct marketing could be broken into separate privacy preferences for contact by telephone, direct mail, electronic mail, and a catchall for "other" action. Further, the scope of the direct marketing could be specified so as to permit only a single contact.

In an alternate embodiment, the security and privacy protection features of the extended database 106 and dataview suite 108 are further enhanced with the use of data encryption. This may be performed by encrypting the data in a given row with an encryption code, or by providing each data field with a unique encryption number. Alternatively, the data may be encrypted at different hierarchical levels of security so as to enforce the privacy preferences of the consumer.

In one embodiment, encryption techniques are used on any identifying field, and selectively applicable on a row basis. This technique allows customers to remain anonymous (e.g. for data mining purposes), but could allow for positive identification for those applications or data requestors that have data encryption rights.

Operation of Dataviews

The dataviews in the dataview suite 108 of the present invention generate SQL statements that selectively pull appropriate columns and rows from the base tables into the result table. Compared to conventional techniques (which materialize entire tables before narrowing the data down to a view subset), this technique reduces the processing required to present the data to the data requestor.

Audit Interface

The owner of the database or an independent auditing service such as BBB ONLINE, TRUSTE, PRICE-WATERHOUSE, TRW, DMA, or CPA WEBTRUST, or NCR may inexpensively run periodic or complaint-driven reviews of the installation. These reviews examine the logical data model and database schema, applications and users that exist for the system, and a TERADATA access log.

The logical data model review examines the dataview structure to confirm the existence of "Standard" Views for Normal users (restricting access to personal information), "Anonymizing" Views for analytic applications, and "Opt Out" Views for other applications.

The applications and user review examines applications and users and the access rights that have been granted to them. This review confirms that "Class A" privileged applications/users have access rights to the "Persona Data" dataview, that "Class B" analytic applications/users have access rights to "anonymizing" dataviews, that "Class C" action-taking applications/users have access rights to "Opt-out" views, that applications that create output tables or files of personal data have access rights to the "Opt Out" and "Anonymizing" Views, and that other applications use the "Standard" View.

Finally, the TERADATA access log or similar log from another database management system is reviewed to assure that the access activity that has occurred complies with the privacy parameters set forth by the data source.

FIG. 4 is a diagram presenting an overview of the operation of a privacy auditing features of the present invention. Whenever a data requesting entity desires access to data in the extended database 106, a request is made to the database management system interface 109 which controls access to the data within the database tables in accordance with privacy parameters. Using a dataview provided from the dataview suite 108 to the requesting entity in accordance with the requesting entity's status as described herein, extended database 106 table is accessed, and the data is provided. At the same time, the database access (or attempted access, if the access is unsuccessful) is logged in an access log 402. Access log 402 includes information regarding the type of access or attempt, the text (SQL) of the request resulting in the access, the frequency of access, the action requested, the name or identification of the requesting entity or application, and the referenced objects (tables, dataviews, and/or macros). The access log 402 permits all accesses to the dataviews in the dataview suite 108, macros in the macro suite 111, or to base tables in the extended database 106 can be audited. All activities granting or revoking access privileges can be audited as well. This is made possible because the access log 402 contents and the table/dataview/macro definitions allow a determination of whether the privacy rules have been enforced or broken.

Privacy audit module 118 is provided to perform a privacy analysis of the data in the access log 402 to validate enforcement of the privacy parameters. The privacy audit module 118 traces all events related to privacy, summarizes activity relating to the access to personal data, and flags any suspected breaches of privacy rules. Privacy test suite 404 comprises programs and other procedures that attempt to "break" the privacy rules, and then examine the access log 402 to determine if privacy rules were enforced or breached. The privacy audit module 118 can be tailored for use by third party auditors who conduct an independent assessment of the enforcement of customer privacy preferences, or by for use by the data warehouse manager.

Metadata Services

Metadata services include a privacy metadata subsystem (PMDS) extension 114. The PMDS extension 114 stores and tracks a number of parameters, and uses these parameters to track activity relating to privacy. Tracked parameters include: (1) data descriptions of all data elements currently in the system (including databases, users, tables, views and macros); (2) data descriptions of internal elements that were source to the system; (3) data descriptions of external elements that were source to the system; (4) data descriptions of internal elements that were target of the system; (5) data descriptions of data elements that were exported from the system; (6) profiles of all users, groups and applications and their access rights to the data; (7) logging of events relating to data access/update, creation of tables/views/macros, granting/revoking of privileges, changes in user profiles, and triggers.

The PMDS extension 114 also stores and manages executable business rules that govern the data controller's adherence to privacy and the logging of events relating to manipulation of the TERADATA logs (e.g. BEGIN/END LOGGING) or similar logs in another DBMS.

The PMDS extension 114 also provides a high-level GUI 406 to for the privacy administrator to review and manage privacy-related metadata. This will include a graphical representation of the databases and their table/view macro structure for all customer (consumer or data subject) information, and of the associated user/user group privileges. The GUI 406 also provides a parameter-driven means of setting up privacy rules and generating consequent dataviews, macros, or access rights, based on definitions provided by the privacy administrator through the GUI 406. The GUI 406 also provides a facility to guide an outside auditor through a review of the site's privacy implementation.

The PMDS extension 114 also provides a reporting facility, which analyzes the contents of the various database and PMDS logs to report on privacy-related activity. The privacy administrator may review such privacy reports via an interactive interface or printed report. Independent auditors, in conjunction with the privacy administrator, may perform their audits with the assistance of such reports.

The PMDS extension 114 also provides a separate GUI application/utility to support consumers in access, review and correction of their personal data and related

privacy rules, and may also provide additional logging facilities to provide more details pertaining to privacy related events.

Macros

Either alone or in combination with the dataviews described herein, macros 111 or stored procedures in the database management system interface can be used to control and log accesses to data. Where macros are used to enforce data privacy parameters, users are not given "select" access rights. Instead, users are given the right to access a macro in the macro suite 111 that performs the actual data access and logs the event in the access log 402 for future auditing purposes. Even so, the macros execute against the data through the same views that restrict access to opted-out rows and columns. Such macros are especially appropriate for recording single-row accesses.

Data Dictionary

The data dictionary 408 stores information about the database schema, including all tables, dataviews and macros in the system, all macros in the system, all users and their privileges (including the privileges of users owning macros).

Process

FIG. 5 is a flow chart illustrating exemplary operations used to practice one embodiment of the present invention. The process begins by accepting a request for a consumer privacy card such as a loyalty card 138 or a smart card 136 from a consumer. This can be accomplished via an Internet 126 connection, through a modem 130, a telephone 132, or a kiosk or ATM 134. This is illustrated in block 502. Then, the consumer is queried 504 for consumer personal information (such as the consumer's name, address, and telephone number), and the consumer's privacy preferences as set forth above. The consumer then enters the requested information. A customer-unique proxy identifying the customer is then generated, associated with the consumer's personal information, and stored in the data warehouse 102. This is depicted in block 506. A privacy card, which manifests the customer privacy preferences, is then issued 508 to the consumer. The

privacy card may be a smart card with memory and limited processing and I/O capability, or may simply be a card with a bar code.

FIG. 6 is a flow chart illustrating exemplary operations performed to store a customer-unique proxy identifying the customer in the data warehouse. First, a proxy is generated, as shown in block 602. Then, the generated proxy is stored in the data warehouse 102 and the privacy card, as shown in blocks 604 and 605.

FIG. 7 is a flow chart illustrating exemplary operations performed to store a customer unique proxy identifying the customer in the data warehouse where the privacy card is a simple loyalty card with a read-only capability such as a barcode. In this embodiment, a pre-stored proxy is read from the card (i.e. the bar code on the card), and transmitted and stored in the data warehouse. This is illustrated in blocks 702 and 704, respectively. Alternatively, the barcode or other manifestation of the proxy can be printed at the kiosk or ATM 134, or by a printer attached to the consumer's computer.

FIG. 8 is a flow chart illustrating exemplary operations performed in participating in a commercial transaction using the privacy card. First, a request for a transaction, which includes the consumer's unique proxy, is received from the consumer, as shown in block 802. The consumer completes the transaction, and the data about the transaction is associated the proxy, as shown in block 804. The transaction data is then stored in the data warehouse 102 so that its association with the proxy is maintained, as shown in block 806.

FIG. 9 is a flow chart illustrating exemplary operations performed in using the privacy card to manage the consumer's privacy preferences. First, a request is received and accepted 902 from the consumer to manage the privacy preferences in the data warehouse. This request includes the consumer's proxy, and is typically encrypted to assure security. After the identity of the customer is verified 904, the customer can then view, alter, and otherwise manage the privacy preferences stored in the data warehouse.

As described in the foregoing operations, a consumer may sign up for a privacy card at an ATM-like self-service kiosk machine 134 in a retail establishment. The machine queries the consumer about various privacy preferences, collects his/her name, telephone numbers, and mailing address, and issues a universal privacy card that can be used immediately in any participating establishment to gain access to special treatment (e.g.

"frequent shopper") privileges, special discounts, and bonus points (e.g. "frequent flyer miles").

By interacting with the kiosk 134, the consumer is able to trade off privacy for special benefits at a detailed level. For example, the consumer can say that they wants a particular "junk mail" flyer or catalog, but not another. Or that the consumer is willing to be called at home by a particular type of store, or a particular store, but only during certain hours. In other words, the privacy card puts the consumer in complete control over what data is collected, and what is done with the data. All privacy preferences are changeable at any time, with complete assurance by the consumer that the new preferences will be adhered to. Furthermore, the consumer does not need to trust every retail establishment to follow the privacy preferences – the consumer must only trust the privacy protection service bureau that issues the card and tracks the consumer's preferences. Finally, since the privacy card works in any participating establishment, the consumer need only carry one card and administer one privacy preference profile.

The foregoing allows retailers to meet the consumers preferences, instead of irritating customers with unwanted junk mail, unwanted phone calls, spam, etc. Furthermore, retailers are able to save significant cost in avoiding mass-mailings and unneeded telephone calls. Lastly, the retailer may perform detailed analyses on the shopping patterns of their most loyal customers, without running any risk of violating their privacy desires or rights. Coupled with automatic recognition systems, a retailer can even sense when a customer enters a retail outlet and determine to what degree that customer wants to be greeted by name left anonymous, or whether they prefer help or to walk the store uninterrupted.

Since the foregoing system puts the consumer in charge of their own privacy, with assurance that the retailers are unable to circumvent the consumers preferences, there is no need for regulatory or legal controls over data mining, junk mail, outbound telemarketing, or spam.

In one embodiment, the privacy card is a smart card with some amount of memory, some computational ability, and some software on it. When attached to the smart card reader at the retailer's point of sale (POS) station, it generates an id number that is a unique customer identification that is different for each retail establishment, but is consistent

between visits and between individual stores owned by the same retailer. When plugged into a smart card reader in the consumer's home PC, it also generates the same id number when the consumer is interacting with the retailer's web site. A third party – the privacy protection service bureau, can only do mailing address, telephone numbers, and email address the translation between the consumer's id number and their name. Thus, although the retailer can track the buying behavior of that consumer, it never knows who the consumer actually is. If the consumer was willing to fill in demographic data as part of their loyalty card profile, and allow it to be accessible to the retailer, the retailer has access to that as well via the privacy protection service.

When the retailer wished to contact the consumer, either via mail, telephone, or email, it must inform the privacy protection service via a computer protocol. The privacy protection service's computer checks the most recent privacy profile for that consumer, and, if the consumer allows it, forwards the email, sets up the telephone call, or mails the flyer to the consumer.

Alternative Embodiments

FIG. 10 is a block diagram showing an alternative embodiment of the present invention. In this embodiment, two databases are used. The first is an anonymized database 708, storing anonymized data and pseudonyms associated with the data in tables 706 stored therein. The second database is a trusted database 1004, storing tables 1002 relating the pseudonyms with customer identification information. In this approach, the customer's name is stored separately in trusted database 1004. This database is used by the data management system interface 109 to bind the identity of the customer to the pseudonym, and hence to the data stored in the anonymized database 1008. The trusted database also stores the individual's privacy parameters.

Client pseudonyms can be provided to the client by the issuance of a loyalty card 138 or smart card 136, by Internet 126 or on-line communications with a client computer, or by other means. The pseudonym can then be used as a proxy for consumer transactions (thus keeping any data thus collected anonymous). If desired, different pseudonyms can be used for different merchants, or different stores to prevent data mining to ascertain the identity of the customer.

The customer may elect to allow the collection, use, or dissemination of non-anonymous data by selecting data privacy preferences. These preferences are enforced by the data management system interface 109, and are provided by the client using the loyalty card 138, smart card 136, Internet 136, or other communication/data storage method. In one embodiment, an intelligent software agent performs data mining functions to examine customer patterns and to make data privacy parameter suggestions based on the mining results.

In another embodiment, the separate trusted database 1004 and anonymized database 1008 are used in a multi level security privacy system, where the encryption, macros, dataviews, and/ or separate database techniques disclosed herein combined to meet the privacy requirements of different jurisdictions, for different retail outlets, or to accommodate different individual preferences.

FIG. 11 is a diagram showing another alternative embodiment of the privacy data warehouse. As with the other embodiments previously described, access to the data in the database management system 104 is again accomplished via a dataview in the dataview suite 108, or a macro in the macro suite 111. In this embodiment, a privacy metadata services interface 802 comprising the privacy service 150, the client interface module 122, metadata monitoring extensions 114, and the audit interface 118 is also interposed between all accesses to the database management system 104. The privacy metadata services interface 1102 can therefore log and control all access to the database management system 104, the dataviews in the dataview suite 108, and macros in the macro suite 111.

FIG. 12 is a diagram showing an exemplary implementation of dataviews with an interposed privacy metadata services interface. Visibility and access to the data in the customer base tables in the database management system 104 is provided by dataviews and macros 111. The views into the data are represented by the concentric squares shown in FIG. 12. A consumer access macro or consumer view provides the user/consumer with access to a single row of the customer database table containing data about that consumer or data subject. A system assistant 1202 supports the definition and maintenance of the database infrastructure, while a privacy assistant 1204 supports the definition and maintenance of the tables, dataviews, macros, user profiles, logs, and audit reports. As before, routine applications 110A have access to the customer base tables via a standard

view 260, analytic applications 110C have access via an anonymized view in which data that renders the customer identifiable is masked, action (marketing) applications 110D have access via an opt-out view in which entire rows of customer data are omitted, and third party disclosure applications 112 are provided with a dataview which presents only customers who have opted-in, but does not allow access to identifying data. The opt-out/anonymizing dataview can be a separately implemented dataview, or can be implemented applying both the opt-out and anonymizing dataviews.

4 Brief Description of Drawings

FIG. 1 is a system block diagram of an exemplary embodiment of a data warehousing system;

FIG. 2 is a block diagram presenting an illustrative example of the structure of customer tables stored in the privacy-extended customer tables and the database views;

FIG. 3 is a block diagram presenting another illustrative example of the customer tables; and

FIG. 4 is a block diagram presenting an overview of the operation of a privacy auditing features of the present invention;

FIG. 5 is a flow chart illustrating exemplary operations used to practice one embodiment of the present invention;

FIG. 6 is a flow chart illustrating exemplary operations used to store a customer-unique proxy identifying the customer in the data warehouse;

FIG. 7 is a flow chart illustrating another embodiment of exemplary operations used to store a customer-unique proxy identifying the customer in the data warehouse;

FIG. 8 is a flow chart illustrating exemplary operations used to perform a transaction with a loyalty card;

FIG. 9 is a flow chart illustrating exemplary operations used to manage the customer's privacy preferences with a loyalty card;

FIG. 10 is a diagram showing an alternative embodiment of the privacy data warehouse with a separately deployed trusted database;

FIG. 11 is a diagram showing an alternative embodiment of the privacy data warehouse with a privacy metadata services interface interposed to manage and log all data access; and

FIG. 12 is a diagram showing an exemplary implementation of dataviews with an interposed privacy metadata services interface.

FIG. 1

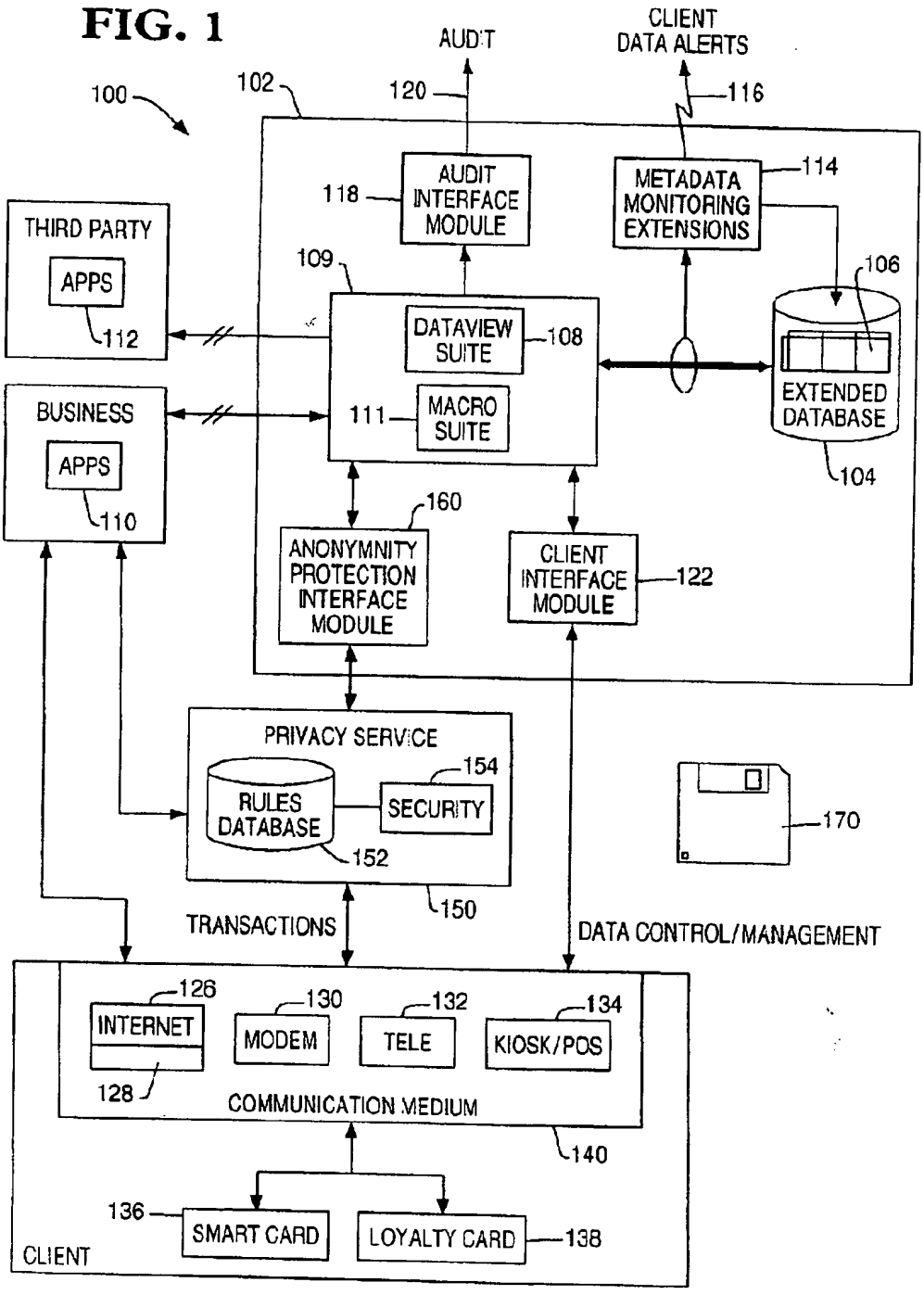

AUDIT
CLIENT DATA ALERTS
100
102
120
116
AUDIT INTERFACE MODULE
118
METADATA MONITORING EXTENSIONS
114
THIRD PARTY
APPS
112
109
106
DATAVIEW SUITE
108
EXTENDED DATABASE
BUSINESS
APPS
110
111
MACRO SUITE
104
160
ANONYMNITY PROTECTION INTERFACE MODULE
CLIENT INTERFACE MODULE
122
PRIVACY SERVICE
154
RULES DATABASE
SECURITY
152
170
150
TRANSACTIONS
DATA CONTROL/MANAGEMENT
126
130
132
134
INTERNET
MODEM
TELE
KIOSK/POS
128
COMMUNICATION MEDIUM
140
136
SMART CARD
LOYALTY CARD
138
CLIENT

FIG. 2A

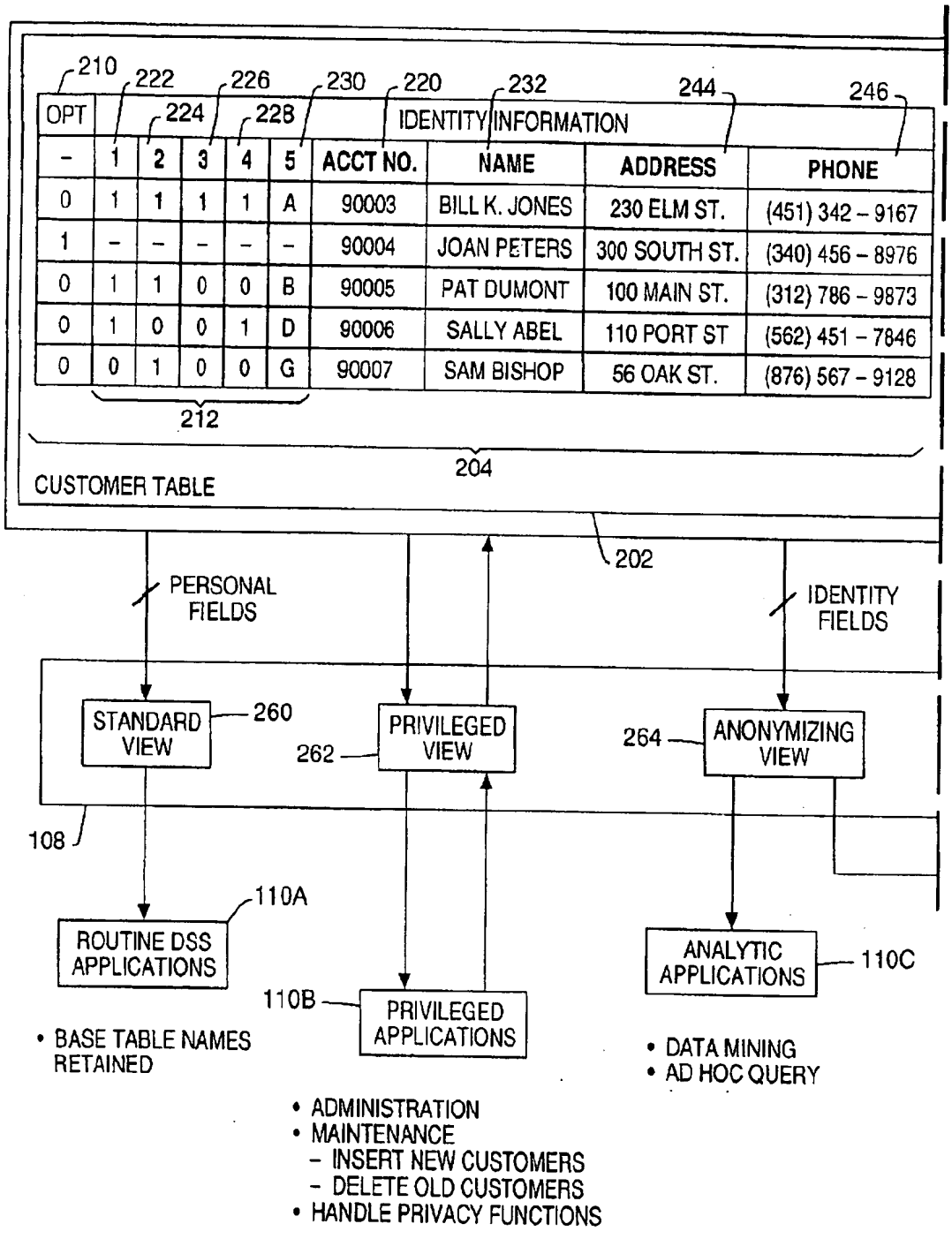

210
222
226
230
220
232
244
246
OPT
224
228
IDENTITY INFORMATION
– 1 2 3 4 5 ACCT NO. NAME ADDRESS PHONE
0 1 1 1 1 A 90003 BILL K. JONES 230 ELM ST. (451) 342 – 9167
1 – – – – – 90004 JOAN PETERS 300 SOUTH ST. (340) 456 – 8976
0 1 1 0 0 B 90005 PAT DUMONT 100 MAIN ST. (312) 786 – 9873
0 1 0 0 1 D 90006 SALLY ABEL 110 PORT ST (562) 451 – 7846
0 0 1 0 0 G 90007 SAM BISHOP 56 OAK ST. (876) 567 – 9128
212
204
CUSTOMER TABLE
202
PERSONAL FIELDS
IDENTITY FIELDS
STANDARD VIEW
260
PRIVILEGED VIEW
262
ANONYMIZING VIEW
264
108
110A
ROUTINE DSS APPLICATIONS
110B
PRIVILEGED APPLICATIONS
ANALYTIC APPLICATIONS
110C
• BASE TABLE NAMES RETAINED
• DATA MINING
• AD HOC QUERY
• ADMINISTRATION
• MAINTENANCE
– INSERT NEW CUSTOMERS
– DELETE OLD CUSTOMERS
• HANDLE PRIVACY FUNCTIONS

FIG. 2B

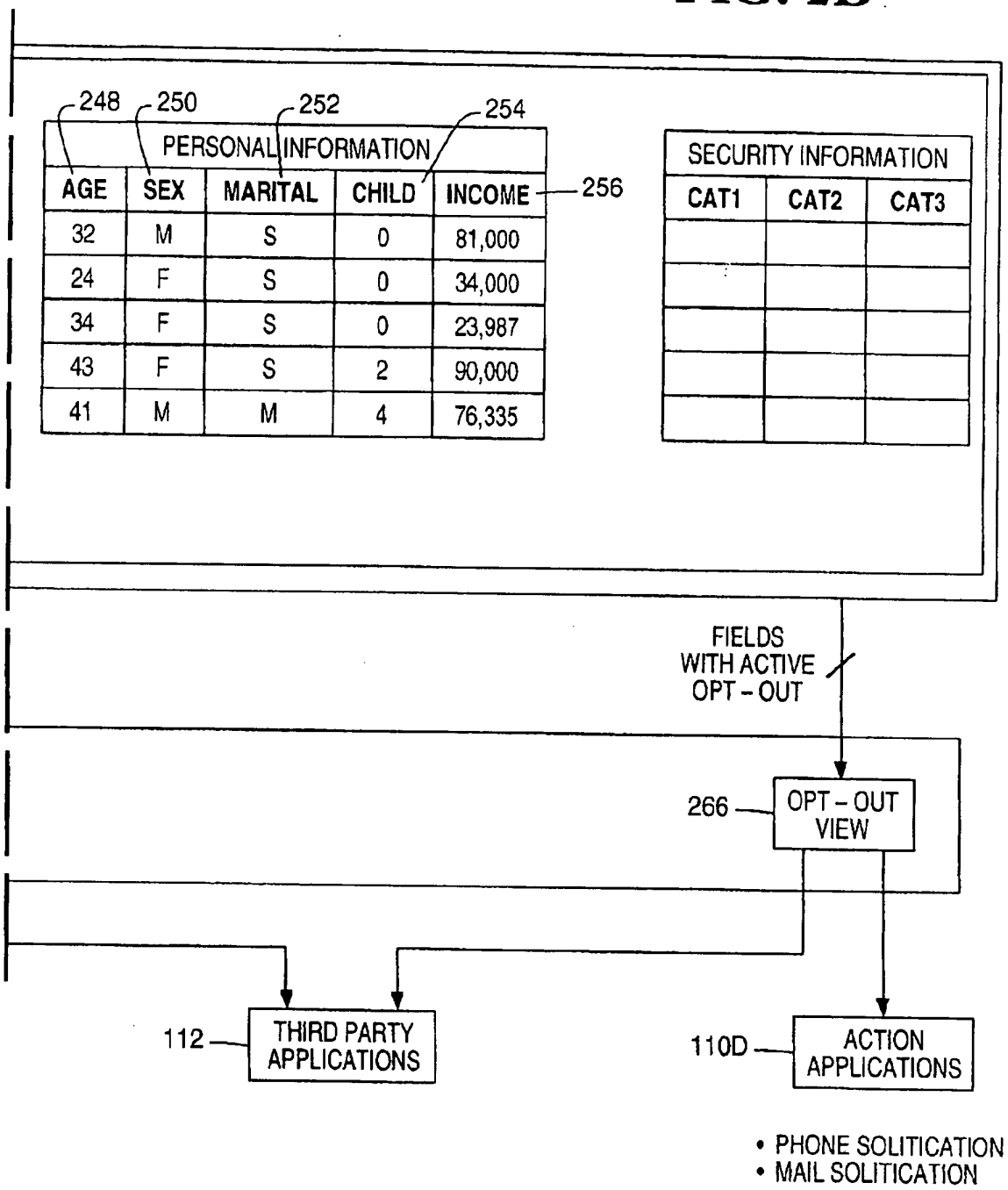

248
250
252
254
PERSONAL INFORMATION
AGE
SEX
MARITAL
CHILD
INCOME
256
32 M S 0 81,000
24 F S 0 34,000
34 F S 0 23,987
43 F S 2 90,000
41 M M 4 76,335
SECURITY INFORMATION
CAT1
CAT2
CAT3
FIELDS WITH ACTIVE OPT - OUT
266
OPT - OUT VIEW
112
THIRD PARTY APPLICATIONS
110D
ACTION APPLICATIONS
• PHONE SOLITICATION
• MAIL SOLITICATION

FIG. 3A

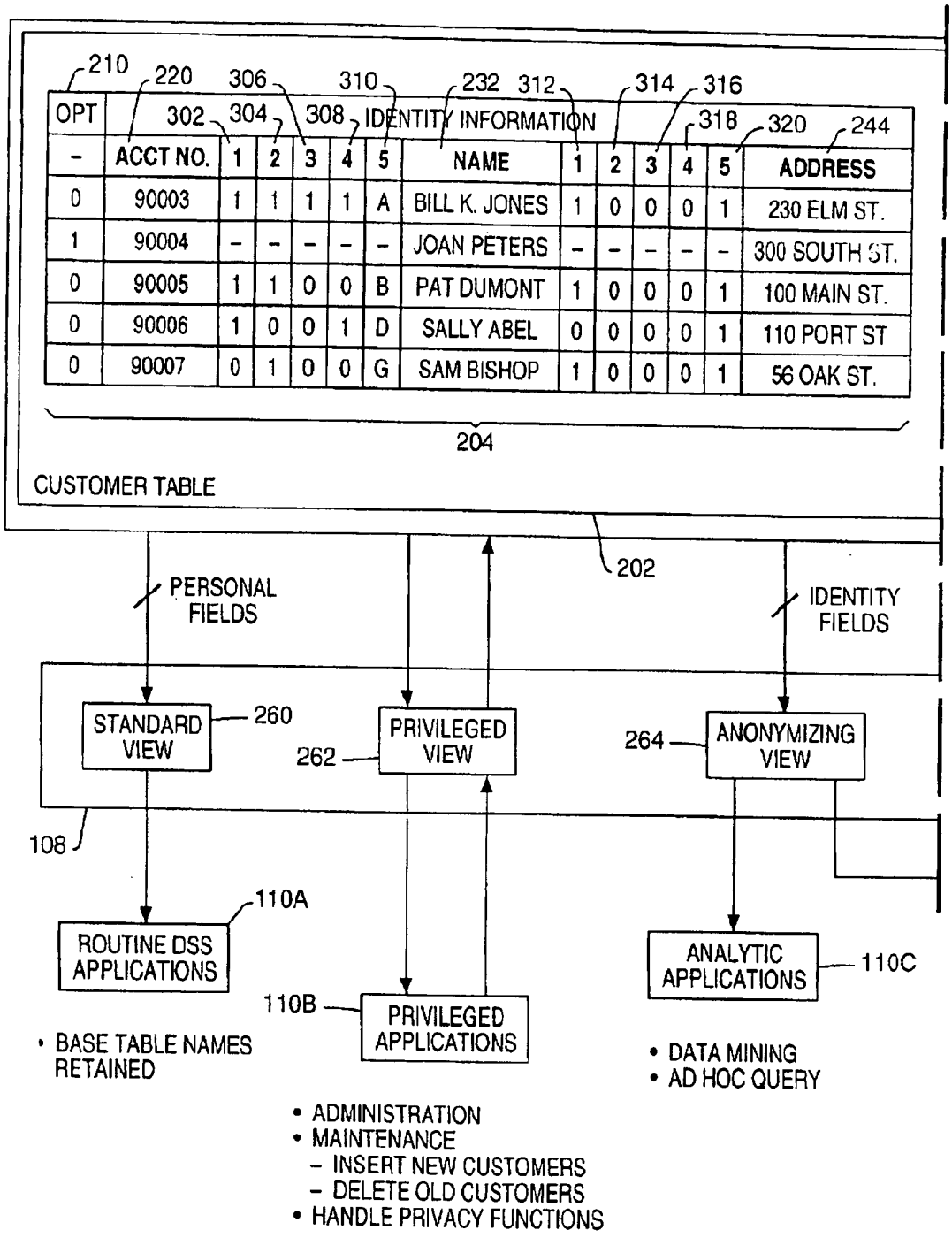
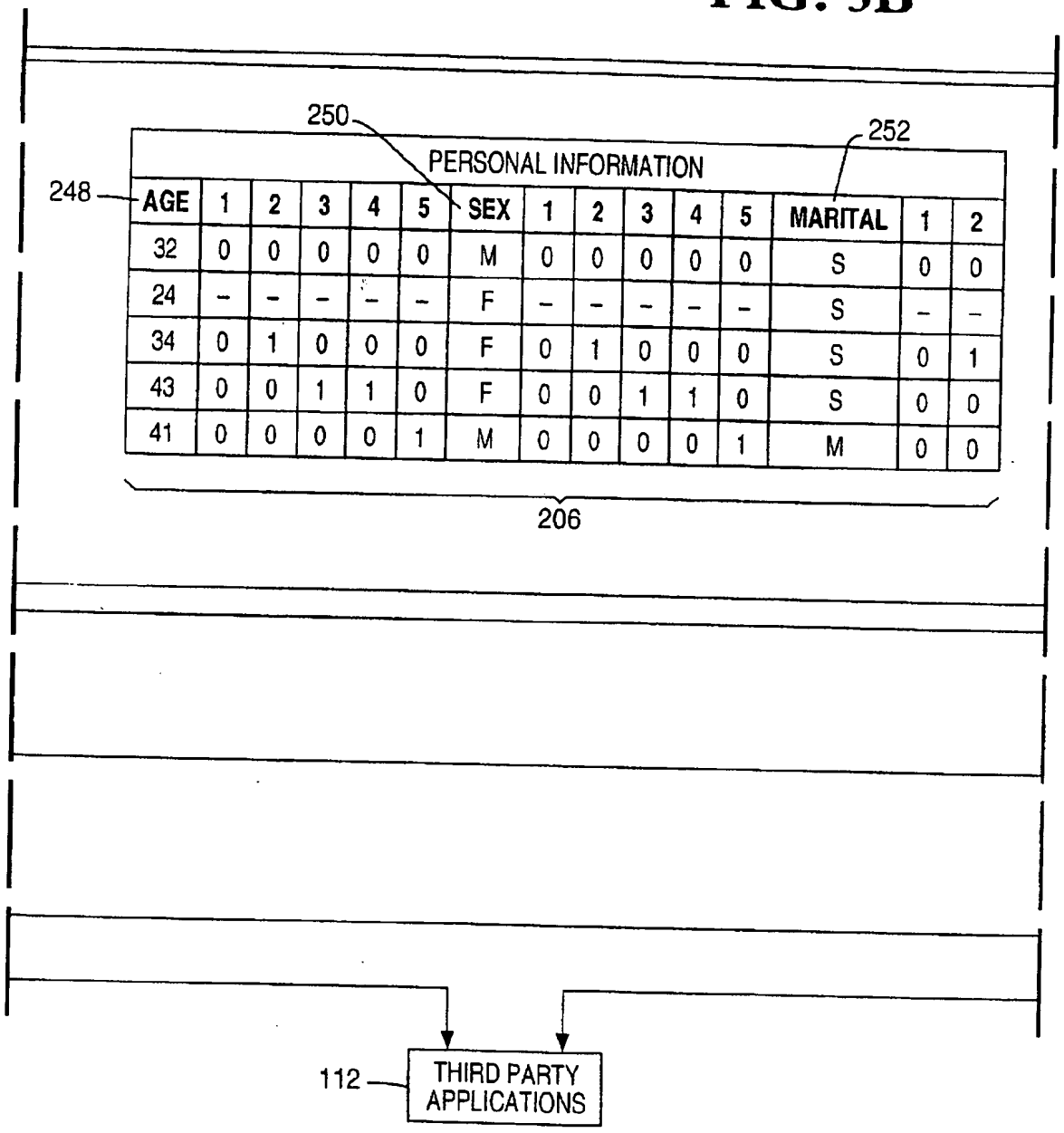

210
220
306
310
232
312
314
316
318
320
244
302
304
308
IDENTITY INFORMATION
OPT
ACCT NO.
1 2 3 4 5
NAME
1 2 3 4 5
ADDRESS
0 90003 1 1 1 1 A BILL K. JONES 1 0 0 0 1 230 ELM ST.
1 90004 - - - - - JOAN PETERS - - - - - 300 SOUTH ST.
0 90005 1 1 0 0 B PAT DUMONT 1 0 0 0 1 100 MAIN ST.
0 90006 1 0 0 1 D SALLY ABEL 0 0 0 0 1 110 PORT ST
0 90007 0 1 0 0 G SAM BISHOP 1 0 0 0 1 56 OAK ST.
204
CUSTOMER TABLE
202
PERSONAL FIELDS
IDENTITY FIELDS
STANDARD VIEW
260
PRIVILEGED VIEW
262
264
ANONYMIZING VIEW
108
110A
ROUTINE DSS APPLICATIONS
110B
PRIVILEGED APPLICATIONS
ANALYTIC APPLICATIONS
110C
• BASE TABLE NAMES RETAINED
• DATA MINING
• AD HOC QUERY
• ADMINISTRATION
• MAINTENANCE
- INSERT NEW CUSTOMERS
- DELETE OLD CUSTOMERS
• HANDLE PRIVACY FUNCTIONS

FIG. 3B



AGE	1	2	3	4	5	SEX	1	2	3	4	5	MARITAL	1	2
32	0	0	0	0	0	M	0	0	0	0	0	S	0	0
24	–	–	–	–	–	F	–	–	–	–	–	S	–	–
34	0	1	0	0	0	F	0	1	0	0	0	S	0	1
43	0	0	1	1	0	F	0	0	1	1	0	S	0	0
41	0	0	0	0	1	M	0	0	0	0	1	M	0	0

FIG. 3C

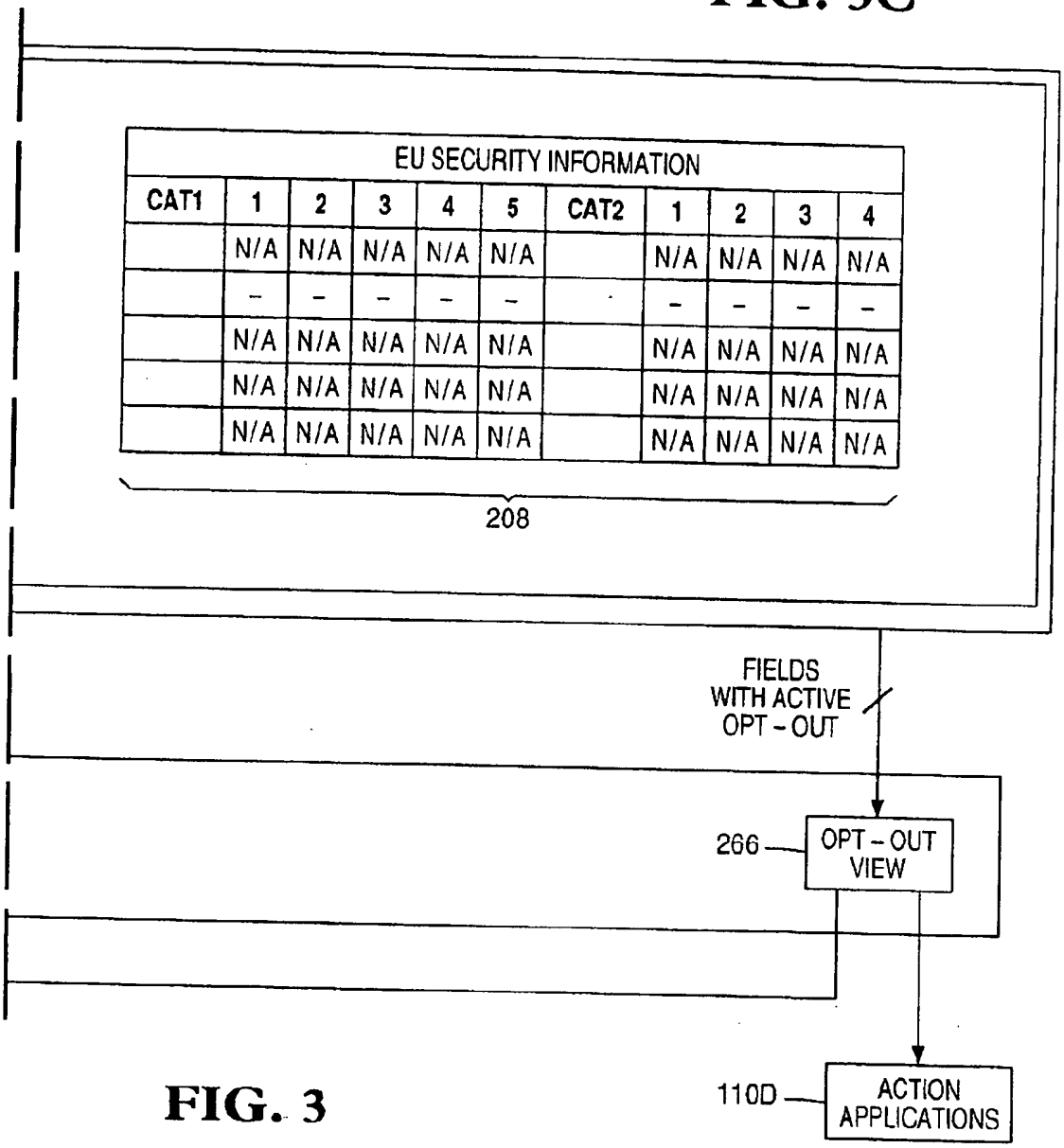


FIG. 3

FIG. 3A	FIG. 3B	FIG. 3C

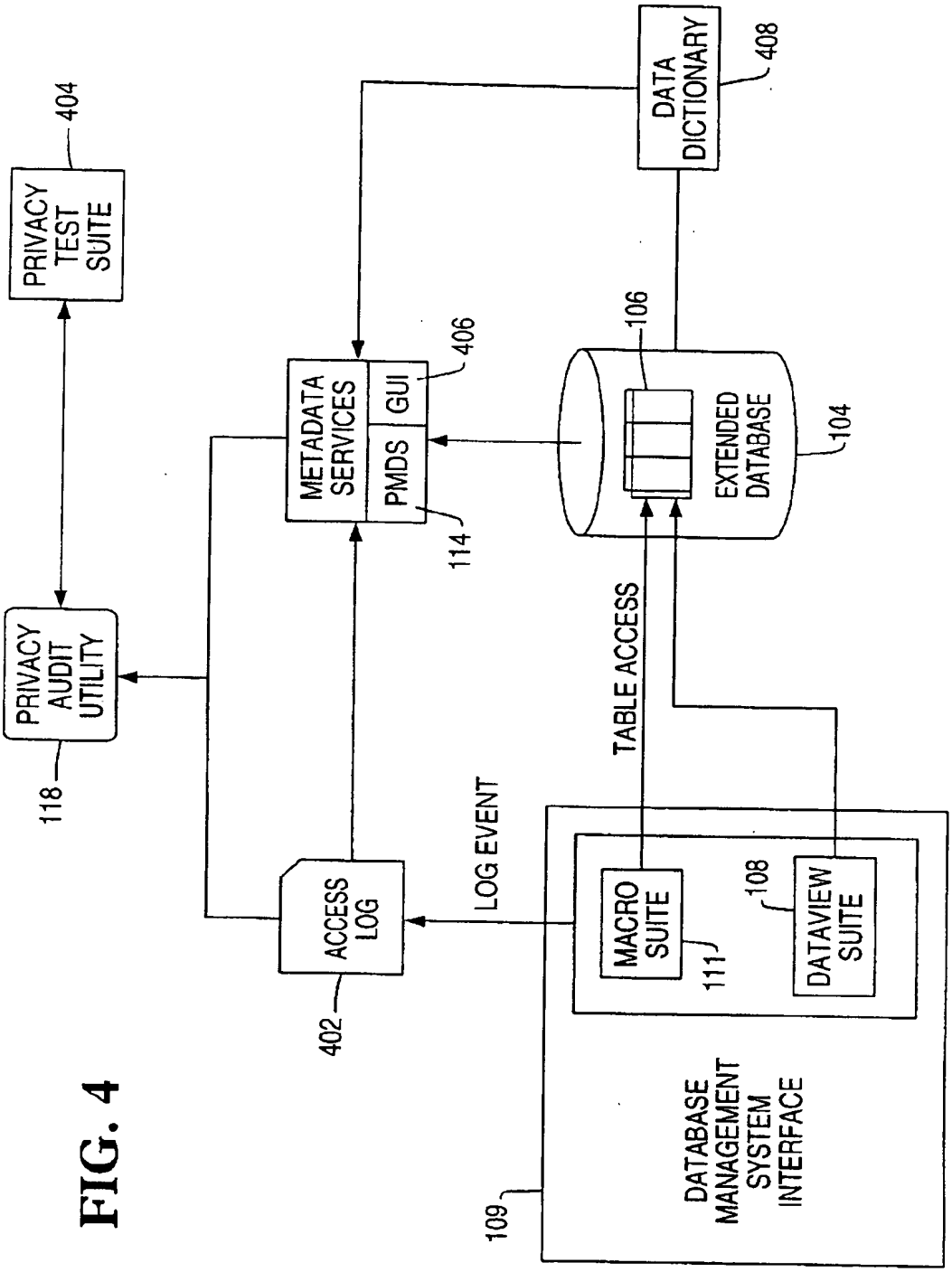

PRIVACY TEST SUITE
404
DATA DICTIONARY
408
METADATA SERVICES
GUI
PMDS
406
114
106
EXTENDED DATABASE
104
PRIVACY AUDIT UTILITY
118
TABLE ACCESS
LOG EVENT
ACCESS LOG
402
MACRO SUITE
111
108
DATAVIEW SUITE
DATABASE MANAGEMENT SYSTEM INTERFACE
109

FIG. 4

FIG. 5

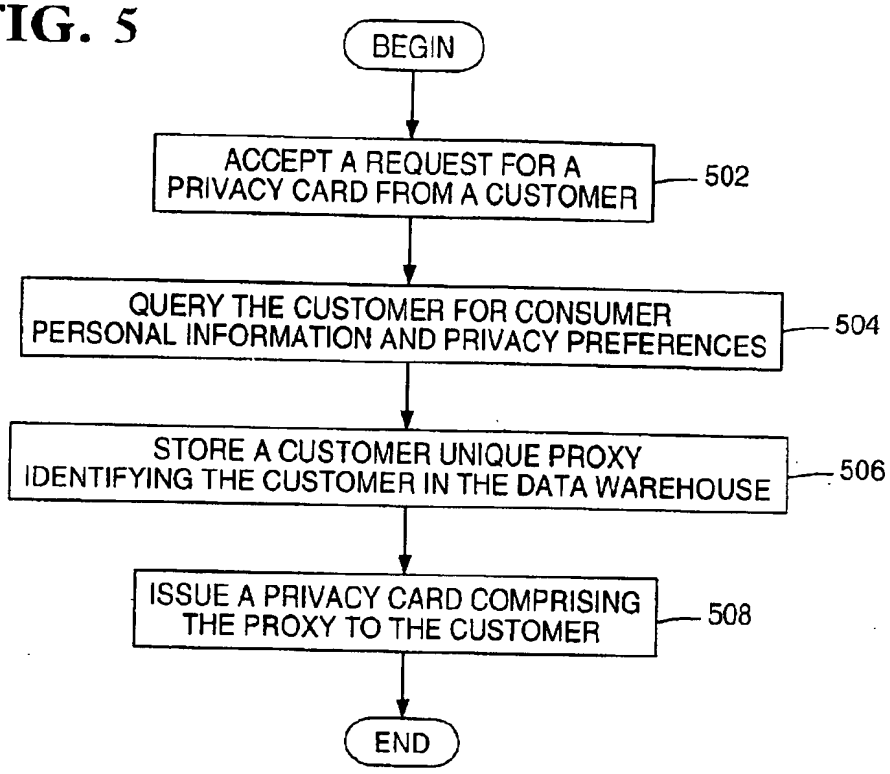

BEGIN
ACCEPT A REQUEST FOR A PRIVACY CARD FROM A CUSTOMER
502
QUERY THE CUSTOMER FOR CONSUMER PERSONAL INFORMATION AND PRIVACY PREFERENCES
504
STORE A CUSTOMER UNIQUE PROXY IDENTIFYING THE CUSTOMER IN THE DATA WAREHOUSE
506
ISSUE A PRIVACY CARD COMPRISING THE PROXY TO THE CUSTOMER
508
END

FIG. 6

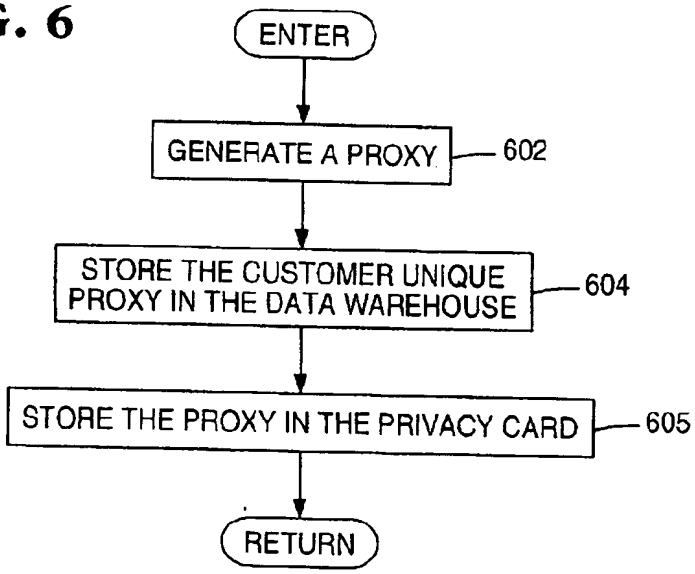

ENTER
GENERATE A PROXY
602
STORE THE CUSTOMER UNIQUE PROXY IN THE DATA WAREHOUSE
604
STORE THE PROXY IN THE PRIVACY CARD
605
RETURN

FIG. 7

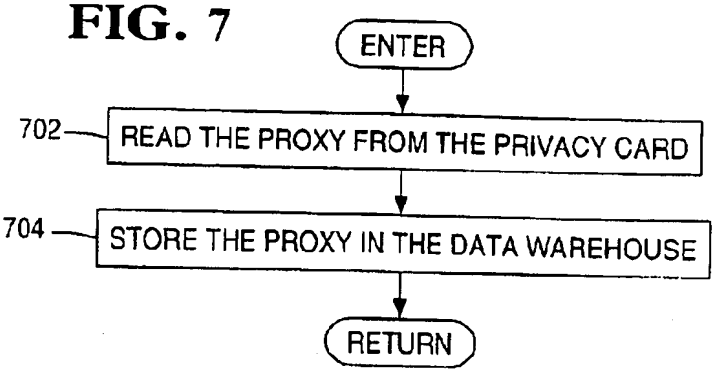


FIG. 8

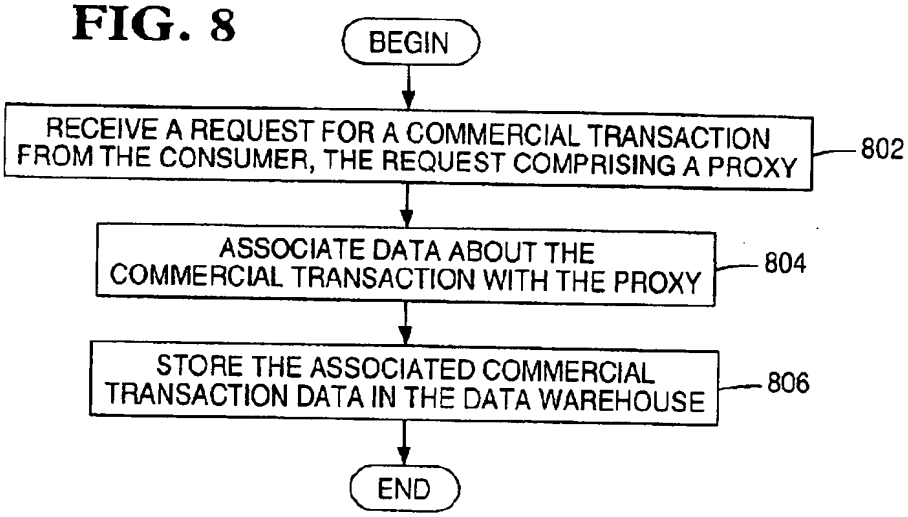


FIG. 9

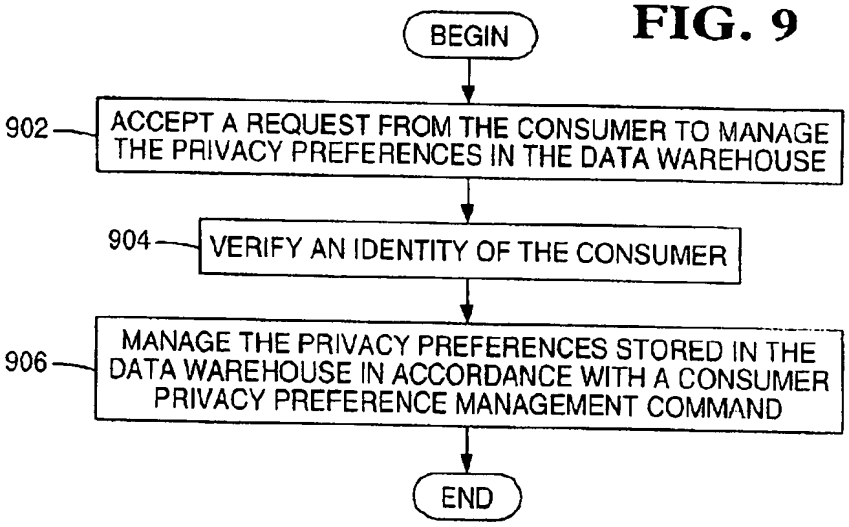


FIG. 10

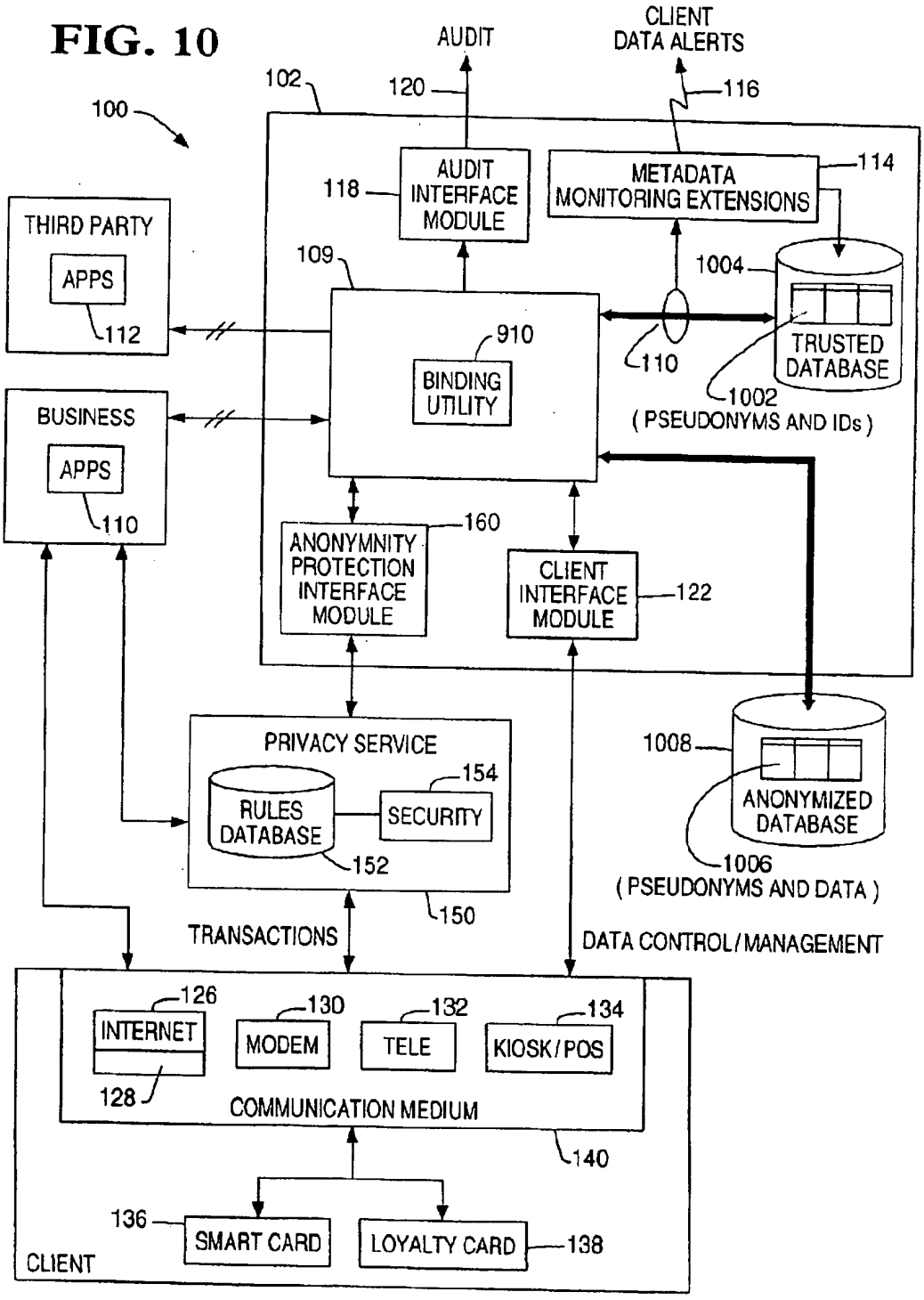

AUDIT
CLIENT DATA ALERTS
102
120
116
100
AUDIT INTERFACE MODULE
118
METADATA MONITORING EXTENSIONS
114
THIRD PARTY
APPS
112
109
1004
910
BINDING UTILITY
TRUSTED DATABASE
110
1002
(PSEUDONYMS AND IDs)
BUSINESS
APPS
110
ANONYMNITY PROTECTION INTERFACE MODULE
160
CLIENT INTERFACE MODULE
122
PRIVACY SERVICE
RULES DATABASE
154
SECURITY
152
150
1008
ANONYMIZED DATABASE
1006
(PSEUDONYMS AND DATA)
TRANSACTIONS
DATA CONTROL/MANAGEMENT
126
INTERNET
130
MODEM
132
TELE
134
KIOSK/POS
128
COMMUNICATION MEDIUM
140
136
SMART CARD
LOYALTY CARD
138
CLIENT

FIG. 11

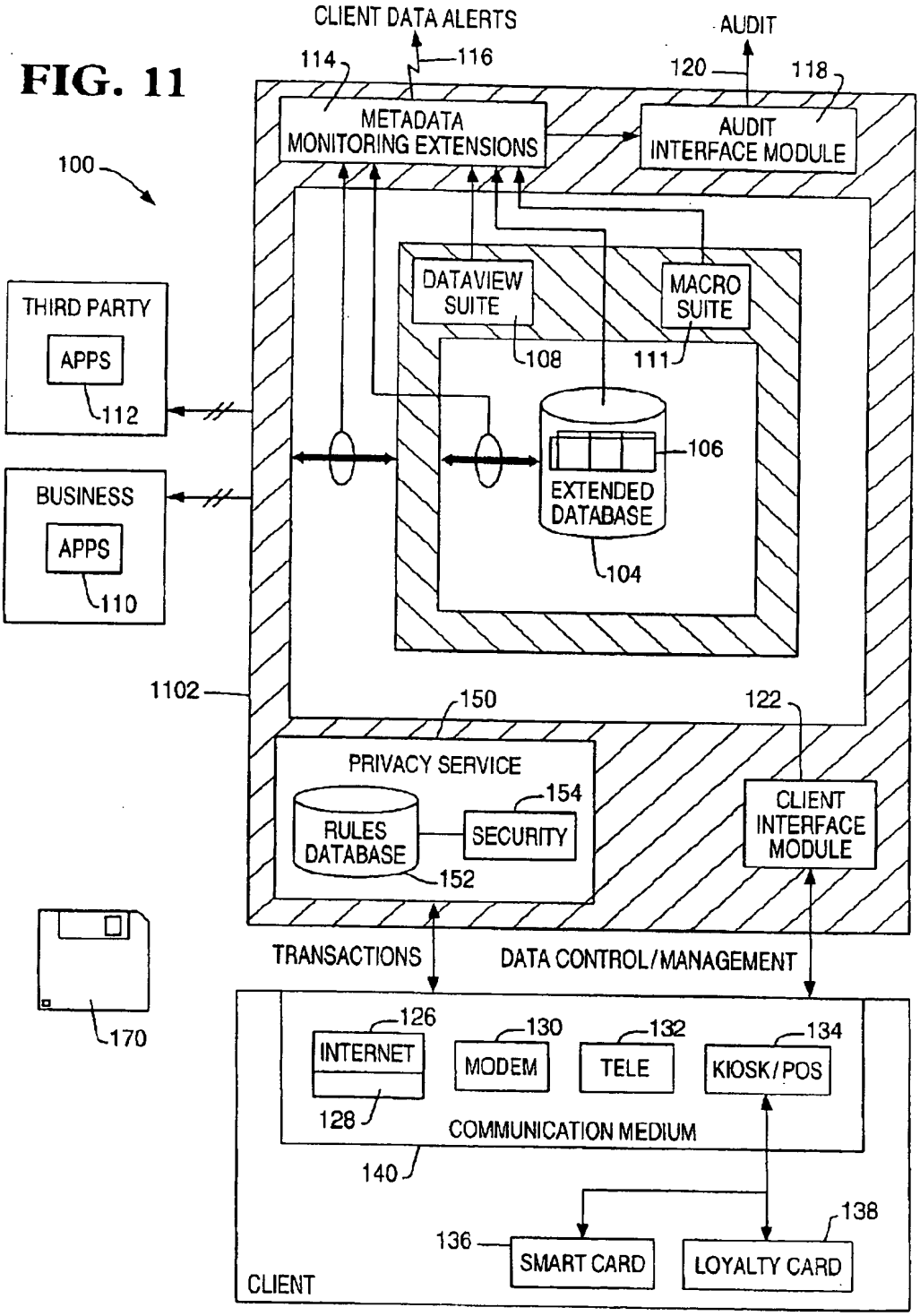
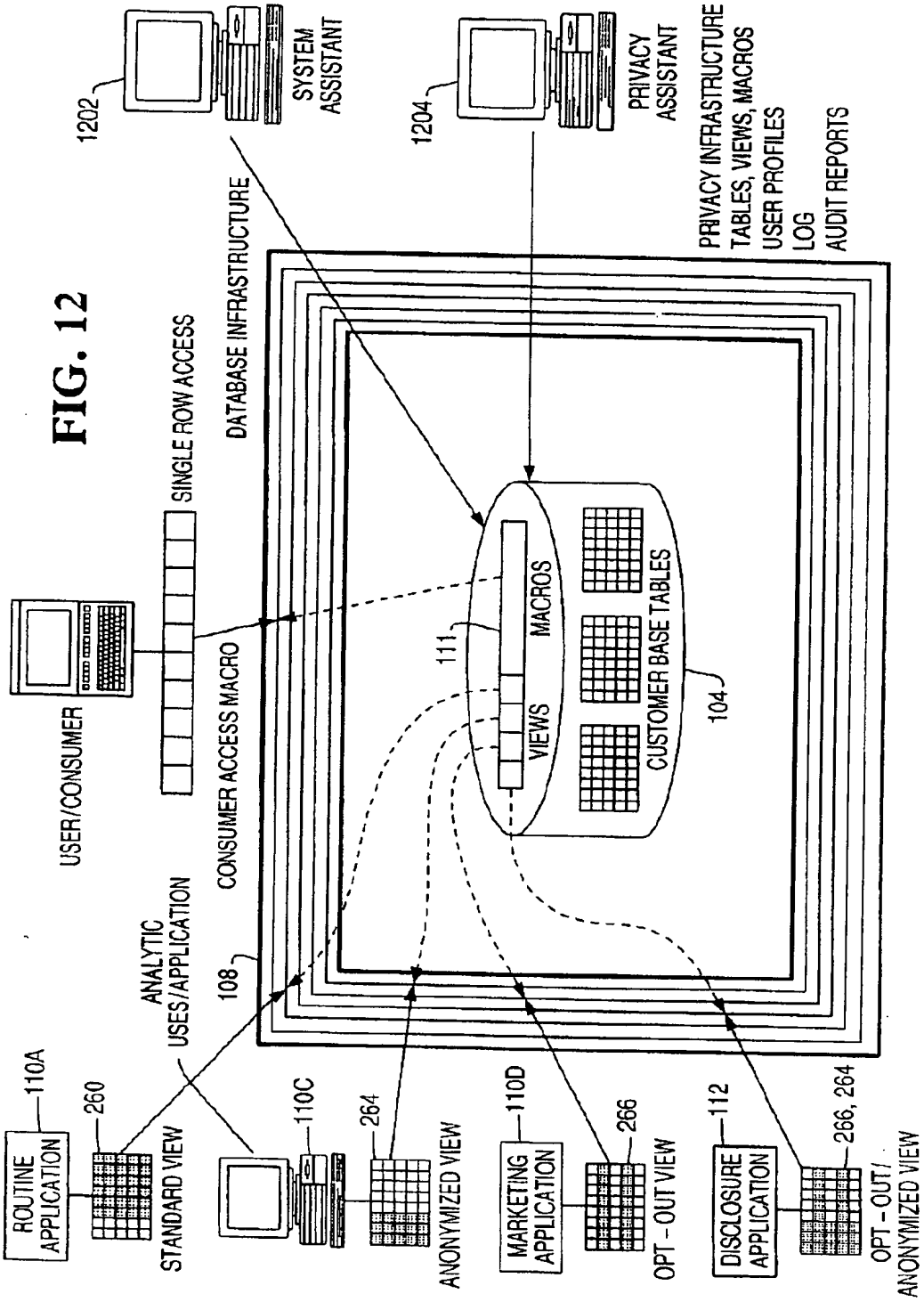

CLIENT DATA ALERTS
AUDIT
114
116
120
118
METADATA MONITORING EXTENSIONS
AUDIT INTERFACE MODULE
100
THIRD PARTY
APPS
112
DATAVIEW SUITE
MACRO SUITE
108
111
106
EXTENDED DATABASE
104
BUSINESS
APPS
110
1102
150
122
PRIVACY SERVICE
154
RULES DATABASE
SECURITY
152
CLIENT INTERFACE MODULE
170
TRANSACTIONS
DATA CONTROL/MANAGEMENT
126
130
132
134
INTERNET
MODEM
TELE
KIOSK/POS
128
COMMUNICATION MEDIUM
140
138
136
SMART CARD
LOYALTY CARD
CLIENT

FIG. 12


1202
SYSTEM ASSISTANT
1204
PRIVACY ASSISTANT
PRIVACY INFRASTRUCTURE TABLES, VIEWS, MACROS
USER PROFILES
LOG
AUDIT REPORTS
DATABASE INFRASTRUCTURE
SINGLE ROW ACCESS
USER/CONSUMER
CONSUMER ACCESS MACRO
111
MACROS
VIEWS
CUSTOMER BASE TABLES
104
108
ANALYTIC USES/APPLICATION
110A
ROUTINE APPLICATION
260
STANDARD VIEW
110C
264
ANONYMIZED VIEW
110D
MARKETING APPLICATION
266
OPT-OUT VIEW
112
DISCLOSURE APPLICATION
266, 264
OPT-OUT/ ANONYMIZED VIEW

1 Abstract

A method, apparatus, article of manufacture, and a memory structure for controlling the collection and dissemination of data stored in a data warehouse is disclosed.

The method comprises the steps of accepting a request for a privacy card from a consumer, querying the consumer for consumer personal information and privacy preferences, storing a customer unique proxy identifying the customer in the data warehouse, and issuing a privacy card comprising the proxy to the customer. The program storage device comprises a medium for storing instructions performing the method steps outlined above. The apparatus comprises a means for accepting the request for a privacy card from the consumer and for querying the consumer for personal information an privacy preferences, such as a kiosk, ATM or internet connection, a data warehouse for storing the customer unique proxy, and a means for issuing the privacy card.

2 Representative Drawing

Fig. 1